

Éditions UNESCO

Organisation
des Nations Unies
pour l'éducation,
la science et la culture

ÉTUDE MONDIALE SUR

LE RESPECT DE LA VIE PRIVÉE SUR L'INTERNET ET LA LIBERTÉ D'EXPRESSION

Par Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin et Natalia Torres

COLLECTION UNESCO SUR LA LIBERTÉ DE L'INTERNET

ÉTUDE MONDIALE SUR

LE RESPECT DE LA VIE PRIVÉE SUR L'INTERNET ET LA LIBERTÉ D'EXPRESSION

Par Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin et Natalia Torres

COLLECTION UNESCO SUR LA LIBERTÉ DE L'INTERNET

Auteurs

- Andrew Puddephatt, directeur, Global Partners & Associates
- Toby Mendel, directeur exécutif, Centre for Law and Democracy
- Ben Wagner, chercheur, Institut universitaire européen
- Dixie Hawtin, chef de projet, Global Partners & Associates
- Natalia Torres, chercheuse, Centre d'études sur la liberté d'expression et l'accès à l'information (CELE) de l'Université de Palermo, Argentine

Conseil consultatif

- Eduardo Bertoni, directeur, Centre d'études sur la liberté d'expression et l'accès à l'information (CELE) de l'Université de Palermo, Argentine
- Gamal Eid, directeur, Réseau arabe d'information sur les droits de l'homme, Égypte
- Sinfah Tunsarawuth, avocat de médias indépendants, Thaïlande
- Sunil Abraham, directeur du Centre for the Internet and Society, Inde
- Grace Githaiga, chercheuse indépendante et Kictanet, Kenya
- Joe McNamee, coordonnateur des actions de plaidoyer, European Digital Rights
- Katitza Rodriguez, directrice pour les droits internationaux, Electronic Frontier Foundation, États-Unis d'Amérique
- Cynthia Wong, juriste, Center for Democracy and Technology, États-Unis d'Amérique

Avec nos remerciements particuliers aux personnes suivantes qui ont bien voulu répondre à nos questions pour cette publication :

Guo Liang, Yang Wang, Ceren Unal, Ang Peng Hwa, Erick Iriarte Ahon, Katitza Rodriguez, Karen Reilly, Ali G. Ravi, Moez Chackchouk, Primavera de Filippi, Peter Parycek, Robert Bodle, Sameer Padania, Peter Bradwell, Ulrike Höppner, Eduardo Bertoni, Hong Xue, Monique Fanjoy, Abu Bakar Munir, Joe McNamee, Amr Gharbeia, Jamie Horsley, Nepomuceno Malaluan, Cynthia M. Wong, Sinfah Tunsarawuth, Prim Ot van Daalen, Sunil Abraham, et un certain nombre d'anciens employés anonymes de grandes sociétés de Technologies.

Publié en 2013 par
L'Organisation des Nations Unies
pour l'éducation, la science et la culture
7 place de Fontenoy, 75352 Paris 07 SP, France

© UNESCO 2013
Tous droits réservés

ISBN 978-92-3-204241-5

Les appellations employées dans cette publication et la présentation des données qui y figurent n'impliquent de la part de l'UNESCO aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites. Les idées et opinions exprimées dans cette publication sont celles des auteurs ; elles ne sont pas nécessairement celles de l'UNESCO et n'engagent pas l'Organisation.

Mis en page et imprimé par l'UNESCO

La traduction et l'impression de cette publication en français ont été rendues possibles par la contribution de l'Agence suédoise de coopération internationale au développement (ASDI)

Imprimé en France

TABLE DES MATIÈRES

AVANT-PROPOS

L'UNESCO, aux termes de son Acte constitutif, promeut « la libre circulation des idées, par le mot et par l'image » et s'est engagée à faciliter la mise en place d'un espace Internet libre, ouvert et accessible dans le cadre de la promotion d'une liberté d'expression complète en ligne et hors ligne.

Comme le démontre la publication de l'UNESCO « Liberté de connexion, liberté d'expression : écologie dynamique des lois et règlements qui façonnent l'Internet », la liberté n'est pas le sous-produit inévitable du changement technique, et il faut la sauvegarder par des mesures législatives et réglementaires appropriées. À une époque de changement rapide, nous sommes pleinement conscients que la liberté d'expression sur l'Internet est complexe et que cela veut dire qu'il faut travailler à trouver un équilibre entre ce droit et d'autres impératifs parfois contradictoires – tels que la sécurité nationale, la protection des droits des auteurs et le respect de la vie privée.

L'UNESCO approche ces questions dans le cadre du processus de suivi du Sommet mondial sur la société de l'information et de nos activités concernant le Forum sur la gouvernance de l'Internet. Nous savons bien que nous vivons aujourd'hui dans un monde où deux milliards d'usagers de l'Internet et de cinq milliards d'usagers du téléphone mobile affichent des millions de blogs, de tweets, d'images et de podcasts publics, ainsi que leurs informations personnelles chaque jour.

Dans ce contexte, l'UNESCO a reconnu que le respect de la vie privée, en tant que droit fondamental, a un impact sur d'autres droits et libertés, dont la liberté d'expression, d'association et d'opinion. Le problème est que les mécanismes destinés à protéger la vie privée en ligne peuvent parfois être utilisés pour porter atteinte à la liberté d'expression légitime en général et au rôle démocratique du journalisme en particulier. Un problème supplémentaire à résoudre pour équilibrer ces droits tient à la discordance des cadres juridiques entre territoires en ligne et hors ligne, ainsi qu'entre compétences nationales et internationales.

Ayant tout cela à l'esprit, la présente publication cherche à identifier la relation entre liberté d'expression et respect de la vie privée sur l'Internet, en déterminant où elles se soutiennent mutuellement et où elles sont en concurrence dans différentes situations. La publication dresse la carte des problèmes dans l'actuel paysage de la réglementation de la protection de la vie privée sur l'Internet du point de vue de la liberté d'expression. Elle offre une vue d'ensemble de la protection juridique, des principes directeurs d'autorégulation, des problèmes normatifs et des études de cas relatives à ce sujet.

En fournissant des informations à jour et pointues sur les questions émergentes intéressant à la fois les pays développés et les pays en développement, nous espérons que cette publication constituera pour les États membres de l'UNESCO et autres parties prenantes un outil de référence utile. De multiples parties prenantes pourront, de préférence dans le cadre d'un dialogue, l'utiliser dans leur propre domaine d'action, en l'adaptant lorsqu'il le faut à partir des diverses expériences mentionnées dans ces pages. La publication

fournit aussi des sources supplémentaires de références aux lecteurs qui souhaiteraient approfondir chacun des sujets évoqués.

Nous voudrions que cette publication contribue à réunir les parties prenantes pour un débat éclairé sur les approches qui favorisent le respect de la vie privée sans compromettre la liberté d'expression. Dans les années qui viennent, l'UNESCO cherchera spécifiquement à diffuser des informations sur les bonnes pratiques et la collaboration internationale concernant les points d'intersection entre liberté d'expression et respect de la vie privée. La recherche sur la sauvegarde du principe de la liberté d'expression dans la politique de l'Internet sur un large éventail de questions restera un élément du mandat normatif de l'UNESCO et de ses conseils techniques aux parties prenantes.

Jānis Kārkliņš
Sous-Directeur général
pour la communication et l'information,
UNESCO

RÉSUMÉ

Le droit au respect de la vie privée est un droit fondamental, bien qu'il soit difficile de définir exactement ce qu'implique ce droit. Il peut être considéré comme ayant un double aspect – il concerne les informations ou la partie de notre vie dont nous pouvons préserver le caractère privé, mais aussi ce que les tiers peuvent faire des informations qu'ils détiennent – les questions de savoir si elles sont protégées, partagées, qui y a accès et dans quelles conditions.

Les interprétations du droit au respect de la vie privée dépendent depuis longtemps des technologies disponibles, les premières questions à ce sujet s'étant posées aux journaux du XIXe siècle. Aussi l'Internet, à son tour, remodèle-t-il inévitablement ce que nous entendons par respect de la vie privée dans le monde moderne.

Le droit au respect de la vie privée sous-tend d'autres droits et libertés, dont la liberté d'expression, la liberté d'association et la liberté de conviction. L'aptitude à communiquer anonymement sans que les gouvernements connaissent notre identité, par exemple, a joué historiquement un grand rôle dans la sauvegarde de la libre expression et le renforcement de la responsabilisation politique, les individus étant plus enclins à s'exprimer sur les questions d'intérêt public s'ils peuvent le faire sans crainte de représailles. Cependant, le droit au respect de la vie privée peut aussi entrer en concurrence avec le droit à la liberté d'expression, et dans la pratique il faut un équilibre entre ces droits. Trouver cet équilibre est une tâche délicate, et qui ne peut être facilement anticipée. C'est pourquoi les tribunaux se préoccupent depuis longtemps de gérer cette relation.

L'Internet pose d'importants nouveaux défis à la protection du droit au respect de la vie privée. En gros, l'Internet :

- Permet de collecter de nouveaux types d'informations – les progrès technologiques ont produit des outils de collecte et de compréhension de types d'information qui dans le passé auraient été impossibles ou impraticables.
- Facilite la collecte et la localisation des informations personnelles – chaque ordinateur, téléphone mobile ou autre appareil connecté à l'Internet possède une adresse IP unique, c'est-à-dire un identificateur unique, ce qui veut dire qu'il est localisable. L'aptitude à localiser tout appareil crée de nouveaux problèmes importants pour le respect de la vie privée.
- Offre aux acteurs publics et privés de nouvelles capacités d'analyse des informations personnelles. L'accroissement de la puissance des ordinateurs signifie que de vastes quantités d'informations, une fois collectées, peuvent être à peu de frais et de manière efficiente stockées, regroupées et analysées. Les progrès technologiques permettent de connecter entre elles les bases de données d'information, ce qui permet de traiter des volumes encore plus grands de données.

- Crée de nouvelles possibilités d'utilisation commerciale des données personnelles. Nombre des services fournis par ces entreprises sont gratuits et leurs modèles d'affaires reposent sur la collecte d'informations sur les utilisateurs et leur utilisation à des fins de marketing.
- Pose de nouveaux défis à la réglementation étant donné la nature transnationale de l'Internet. Malgré l'émergence de normes internationales sur les meilleures pratiques de protection des données, il y a encore beaucoup à faire pour harmoniser les lois nationales. Les entreprises en ligne ont encore du mal à s'orienter dans le dédale complexe des lois nationales sur le respect de la vie privée lorsqu'elles gèrent des services internationaux Internet qui transcendent les frontières nationales, et les ambiguïtés juridiques compromettent la protection de la vie privée.

Diverses menaces sur le respect de la vie privée qui se sont développées au moyen de l'Internet sont examinées plus en détail dans la section 2 de la publication. Les questions suivantes sont explorées :

(1) Les opportunités et les problèmes du maintien du contrôle sur les données personnelles en ligne.

(2) Une série d'initiatives visant à protéger la vie privée et l'anonymat en ligne.

(3) Les rôles et responsabilités des fournisseurs de services et des intermédiaires.

(4) Les problèmes spécifiques posés par différentes applications, plates-formes de communication et modèles d'affaires, dont l'informatique en nuage, les moteurs de recherche, les réseaux sociaux et autres dispositifs divers.

(5) Les problèmes posés par la gouvernance en ligne et autres approches gouvernementales.

(6) Les menaces que représentent différents mécanismes de surveillance et de collecte des données : identificateurs uniques ; cookies (et autres formes connexes d'identification des usagers) ; publiciels ; espiogiciels et logiciels malveillants enregistrent subrepticement des données et pratiquent une surveillance clandestine ; inspection approfondie des paquets (DPI) ; technologie du traitement des données et technologies de reconnaissance faciale et de surveillance.

Les normes juridiques internationales relatives au respect de la vie privée et les réponses à ces questions émergentes sont explorées dans la section 3. Cette section énonce les interprétations et protections explicites du droit au respect de la vie privée dans la réglementation internationale des droits de l'homme. Elle analyse ensuite les lois clés et les cadres réglementaires qui ont un impact sur la protection des droits au respect de la vie privée en ligne aux niveaux régional et national dans les pays à travers le monde, et analyse en outre les points forts et les points faibles de l'autorégulation en tant qu'instrument de la protection de la vie privée – qu'elle soit utilisée comme un mécanisme central ou comme un mécanisme destiné à compléter les protections juridiques.

Les droits au respect de la vie privée et à la liberté d'expression ont une relation complexe. La section 4 explore ces intersections plus en détail. À certains égards, le respect de la vie privée est une condition préalable de la liberté d'expression – cela est spécialement vrai dans les pays où il peut être dangereux de discuter ouvertement de certaines questions (telles que la politique, la religion ou la sexualité). Cependant, il existe

aussi des tensions notables entre les deux droits, par exemple lorsqu'un journal voudrait publier des détails privés sur un politicien éminent, peut-être parce que le journal estime que c'est dans l'intérêt public. Ces tensions sont apparues beaucoup plus évidentes avec les changements massifs de la liberté d'expression résultant de l'Internet et des autres systèmes numériques de communication.

La publication explore le droit international et la pratique de différents États en matière de respect de la vie privée sur l'Internet, en tenant compte des conflits potentiels avec d'autres droits, en particulier la liberté d'expression. La section 5 contient nos recommandations aux États et aux entreprises en vue d'une meilleure pratique, fondées sur nos recherches et nos consultations. Les recommandations couvrent les mesures juridiques et réglementaires (mesures constitutionnelles, protection au titre du droit civil, protection au titre du droit pénal, systèmes de protection des données), la politique des entreprises et l'amélioration des pratiques et de la sensibilisation.

Enfin, la section 6 offre une vue d'ensemble des travaux, des matériels de référence et des outils sur la politique et la pratique internationales et nationales en matière de respect de la vie privée et de liberté d'expression sur l'Internet. Cette section est conçue pour servir de ressource aux lecteurs qui souhaitent accéder à d'autres instruments, outils et informations.

1. INTRODUCTION

La nécessité du respect de la vie privée est profondément ancrée chez les êtres humains. Dans sa forme essentielle, le respect de la vie privée est fondé sur la notion d'intégrité et de dignité personnelle. Toutefois, cela est aussi difficile à définir avec un degré convenu de précision – dans différents contextes, cela englobe le droit à la liberté de pensée et de conscience, le droit d'être seul, le droit de contrôler son propre corps, le droit de protéger sa réputation, le droit à une vie familiale, le droit à une sexualité qu'on a soi-même choisie. De plus, ces notions varient d'un contexte à un autre. En dépit de son ubiquité, il n'y a pas de définition de la vie privée qui soit universellement comprise de la même façon. Dans le monde moderne, la vie privée comporte deux dimensions – premièrement les questions relatives à l'identité d'une personne et deuxièmement la façon dont les informations personnelles sont traitées.

L'idée qu'on se fait de la vie privée est depuis longtemps façonnée par les technologies disponibles. Au niveau le plus évident, le respect de la vie privée implique la limitation des invasions de l'espace physique et la protection du domicile et des biens personnels, raison pour laquelle les premières protections de la vie privée ont été axées sur l'inviolabilité du domicile et de la vie familiale. Les préoccupations concernant les informations détenues sur une personne sont venues avec les technologies de la communication. Les préoccupations causées par l'érosion du respect de la vie privée ne sont pas nouvelles – en fait on pourrait affirmer qu'elles sont une caractéristique du XXe siècle. Le document fondateur de Warren et Brandeis intitulé « The Right to Privacy », en 1890, rédigé à une époque où les journaux imprimaient des images des personnes pour la première fois, définissait le droit comme celui d'être laissé en paix. Leur définition – déterminée par une technologie émergente comme c'est souvent le cas avec la vie privée – se souciait de protéger la « personnalité inviolable » et d'englober des valeurs telles que la dignité individuelle, l'autonomie personnelle et l'indépendance[1]. La croissance des médias modernes et l'accent mis par l'industrie de la publicité sur la compréhension des désirs des consommateurs a conduit Myron Brenton à affirmer que nous vivons à « l'ère de l'aquarium », où les vies privées sont rendues publiques par la manipulation et l'échange des données personnelles[2].

Il y a une tension entre le droit à la liberté d'expression – en particulier l'exercice de ce droit par les médias – et le droit au respect de la vie privée. La liberté d'expression, qu'elle soit exercée par des individus ou par les médias, et l'aptitude à l'exercer sont une caractéristique essentielle de toute société ouverte, libérale et démocratique. Ce n'est qu'en pratiquant la libre expression que les sociétés peuvent maintenir une réelle obligation redditionnelle démocratique. Toutefois, le droit à la liberté d'expression n'est pas illimité et il peut être restreint pour protéger les droits et libertés d'autrui. C'est un exercice d'équilibre délicat de décider où se situe la frontière entre libre expression et respect de la vie privée mais les tribunaux en ont l'habitude.

---

1 Bloustein, E. (1964) Privacy as an aspect of human dignity: an answer to Dean Prosser 39 NYU L Rev 962.

2 Brenton, M. (1964) The Privacy Invaders [traduction française : « Les ennemis de votre vie privée.

Dernièrement, le droit à la vie privée a aussi été défini comme le droit des individus de déterminer quand, comment et dans quelle mesure les informations les concernant sont communiquées à autrui[3] face à la montée en puissance des ordinateurs. Le droit au respect de la vie privée, selon Westin, « est la revendication des individus, des groupes ou des institutions de décider eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées à autrui… C'est le désir des individus de choisir librement dans quelles circonstances et dans quelle mesure ils livrent leur personne, leurs attitudes et leurs comportements à autrui »[4]. La dimension spécifique du respect de la vie privée créée par l'Internet est examinée de plus près dans la section 2, Vue d'ensemble des défis et des opportunités de la protection de la vie privée sur l'Internet.

Les débats sur la vie privée et les technologies de l'information depuis les années 1990 n'ont guère tenu compte du genre. Des préoccupations ont été exprimées au sujet du pouvoir des technologies de l'information invasives de violer la vie privée des femmes à des fins sexuelles et au sujet de la « vie privée forcée » imposée par les cultures patriarcales aux femmes et aux filles. Ces deux problèmes n'occupent une place centrale ni dans les questions abordées dans la présente publication ni dans l'exercice des droits au respect de la vie privée dont il sera question dans les sections suivantes. C'est pourquoi notre étude se réfère partout aux individus au lieu de distinguer entre les femmes et les hommes, car nous estimons que les droits au respect de la vie privée sont universels et applicables de manière égale aux femmes et aux hommes.

De même que les conceptions de la vie privée ont évolué avec les circonstances, les premières formes de protection juridique n'étaient pas des systèmes complets de protection de la vie privée mais tentaient de résoudre des problèmes spécifiques dans des contextes et des situations spécifiques (qui pourraient aujourd'hui être considérés comme des aspects du droit général au respect de la vie privée). Un exemple très ancien d'une telle législation sur la « vie privée » est le Justices of The Peace Act anglais de 1361. Il prévoyait l'arrestation des regardeurs et écouteurs indiscrets[5]. L'arrêt précurseur dans l'affaire Entick c. Carrington [1765] qui a donné forme au Quatrième Amendement de la Constitution des États-Unis a eu pour origine le désir de protéger les documents détenus dans une demeure privée. D'autres exemples étaient centrés sur les fins auxquelles les gouvernements pouvaient utiliser les informations qu'ils possédaient sur les individus (Suède) ou les interdictions de publier certains types d'informations personnelles (France et Norvège)[6].

---

3 Westin A.F. (1967) Privacy and Freedom New York: Atheneum, page 7.

4 Ibid.

5 Beresford A. et Stajano F. (2003) Location Privacy in Pervasive Computing, IEEE Communications Society.

6 Privacy International, (2006) Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments.

Au XXe siècle, les normes juridiques internationales ont défini le droit au respect de la vie privée comme un des droits de l'homme. La Déclaration universelle des droits de l'homme (UDHR) de 1948 contenait la première tentative pour protéger le droit au respect de la vie privée comme un droit humain distinct. L'article 12 de la Déclaration dispose :

> « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Bien que juridiquement non contraignante, la Déclaration s'est révélée détenir une immense autorité et on peut trouver le droit au respect de la vie privée dans de nombreux autres instruments des droits de l'homme, dont le Pacte international relatif aux droits civils et politiques, juridiquement contraignant, et la Convention européenne des droits de l'homme (CEDH). Ces instruments sont traités plus en détail dans la section 3 relative aux normes juridiques, L'environnement juridique et réglementaire de la protection de la vie privée.

Outre ces dispositions internationales à caractère général, de nombreux pays incluent un droit au respect de la vie privée dans leur constitution, lui consacrent des lois spécifiques ou ont fait reconnaître par les tribunaux des droits implicites au respect de la vie privée, comme c'est le cas en Canada, en France, en Allemagne, au Japon et en Inde[7]. Certains services de recensement ont adopté des politiques relatives au respect de la vie privée visant à garantir la protection des informations personnelles collectées[8].

Malgré les protections étendues prévues à la fois dans les constitutions et les lois fondamentales, le droit au respect de la vie privée reste un concept quelque peu nébuleux et l'obtention du droit dépend dans une large mesure des circonstances des cas individuels. La Cour européenne a elle-même jugé que « la Cour ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de « vie privée »[9]. Le manque de clarté a conduit un commentateur à dire que le fait que quelque chose « ne semble pas correct … est souvent l'indication la plus utile d'un démarcage entre une immixtion raisonnable dans la vie privée d'un individu et une immixtion qui ne l'est pas »[10]. Privacy International a tenté d'introduire un peu de clarté en définissant quatre types différents de confidentialité : la confidentialité de l'information (par exemple les données personnelles), l'intimité corporelle, la confidentialité de la communication (par exemple la surveillance) et la territorialité privée (par exemple le domicile)[11]. Pour ce qui est de l'Internet, la confidentialité de l'information et celle de la communication sont les plus pertinentes.

L'importance accordée au respect de la vie privée par tant de législateurs et de penseurs au cours de l'histoire indique son intérêt, cependant, comme le dit Paul Chadwick (commissaire à l'information de l'État australien de Victoria) : « Le respect de la vie privée est la plus tranquille de nos libertés… La vie privée est facilement noyée dans les débats

---

7 Solove, D.J. (2008) Understanding Privacy Harvard University Press.

8 United States Census Bureau, Data Protection and Privacy Policy http://www.census.gov/privacy/data_protection/our_privacy_principles.html

9 Niemietz c. Allemagne (1992), 16 EHRR 97. Par. 29.

10 Hosein, G. (2006) "Privacy as freedom" dans R. Jorgensen (dir. publ.) "Human Rights in the Global Information Society" MIT Press, Cambridge.

11 Privacy International, 2006.

sur les politiques publiques … C'est quand elle est absente et non quand elle est présente qu'elle est le plus valorisée »[12]. La valeur de la vie privée a été exprimée en termes de valeur pour l'individu, elle est indispensable à la dignité humaine et en fait à l'individualité, et on dit que si toutes nos actions sont observées et cataloguées, nous sommes moins capables d'être nous-mêmes. La valeur de la vie privée a aussi été exprimée en termes de son instrumentalité. La démocratie et la liberté reposent sur la possession par les individus d'un certain degré de vie privée. Le droit au respect de la vie privée sous-tend de nombreux droits de l'homme, le droit à la liberté d'association, la liberté de conviction et la liberté d'expression étant des exemples particulièrement significatifs. Comme le dit un auteur, « en un sens, tous les droits de l'homme sont des aspects du droit au respect de la vie privée »[13] car si la vie privée est protégée, l'intégrité de l'individu est garantie et c'est le fondement des autres droits et libertés destinés à protéger la dignité de la personne.

Toutefois, il faut aussi noter que si les gens se préoccupent souvent de la protection de la vie privée dans l'abstrait, ils semblent moins soucieux de cette protection dans la pratique. Il ressort clairement d'une utilisation superficielle de l'Internet que les gens livrent des informations personnelles dans des proportions souvent surprenantes. Beaucoup d'auteurs ont remarqué l'écart entre ce que les gens disent qu'ils valorisent et ce qu'ils font réellement en ligne. Cela s'explique peut-être par la nature de l'Internet, auquel on accède souvent en privé et qui est à la fois un moyen de communication sous la forme du courriel (ce qui peut suggérer à l'usager le caractère privé d'un appel téléphonique ou d'une conversation privée) et un moyen public comme avec une application telle que Facebook. Certaines observations empiriques indiquent que les gens ne réalisent pas les implications de la publication en ligne, de la façon dont elle sera mondialement disponible et impossible à supprimer. Par exemple, 57 % des adultes aux États-Unis qui utilisent l'Internet chez eux croient à tort que lorsqu'un site Web a une politique de confidentialité, il ne communiquera pas leurs informations personnelles à d'autres sites Web ou entreprises[14].

1.1 Comment l'Internet a-t-il modifié la nature des menaces sur la vie privée ? Quelles sont les principales menaces de l'ère numérique ?

L'accès à l'Internet se développe rapidement presque partout dans le monde. Les statistiques de l'UIT, Figure 1, montrent que rien qu'entre 2005 et 2010, le nombre d'usagers de l'Internet a doublé. En 1995, 0,4 % seulement de la population mondiale avait accès à l'Internet, et en mars 2011 ce pourcentage atteignait 30,2 %[15]. Cela correspond à plus de deux milliards d'usagers de l'Internet, dont 1,2 milliard dans les pays en développement. La progression de l'utilisation des téléphones mobiles a été encore plus extraordinaire. La Figure 2 montre le nombre d'abonnements à la téléphonie mobile en 1998 et 2009. Aujourd'hui, il y a dans le monde 5,3 milliards d'abonnements

---

12 Ibid., page 2.

13 Volio, F. "Legal Personality, Privacy and the Family" dans Henkin (dir. publ.), The International Bill of Rights (Columbia University Press 1981).

14 Turow, J. Americans and Online Privacy: The System is Broken http://www.securitymanagement.com/archive/library/Anneberg_privacy1003.pdf

15 Internet World Statistics http://www.internetworldstats.com/emarketing.htm

à la téléphonie mobile. Les réseaux mobiles sont accessibles à 90 % de la population mondiale et certains commentateurs estiment que l'accessibilité universelle sera réalisée dans les cinq années à venir[16]. Dans les pays développés, il y a plus d'abonnements à la téléphonie mobile que d'habitants (113,6 abonnements pour 100 habitants), et bien que le nombre d'abonnements soit bien inférieur dans les pays en développement, il est tout de même très élevé, avec 56,6 abonnements pour 100 habitants[17].



Figure 1[18] Internautes par région

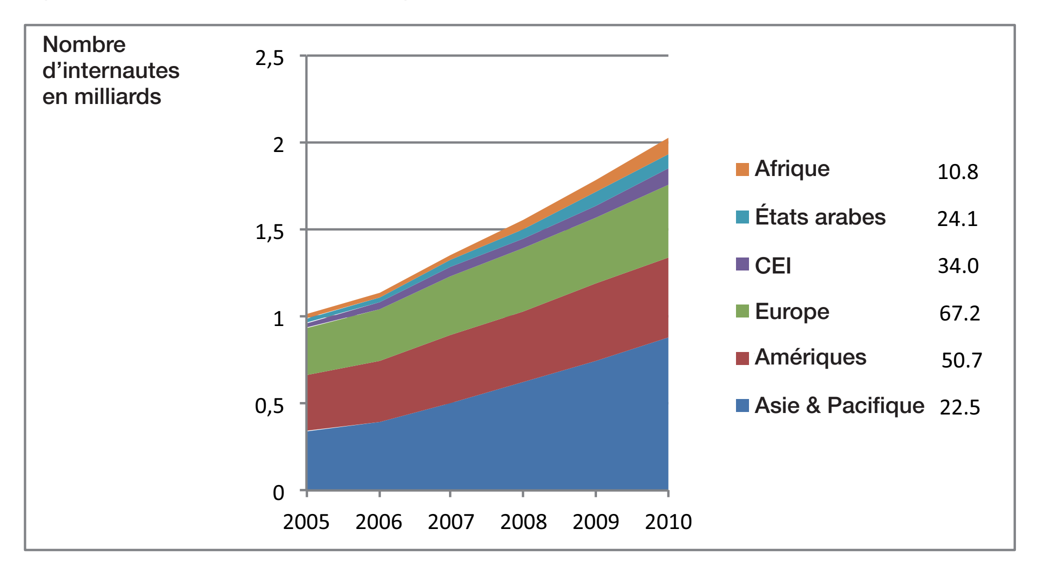
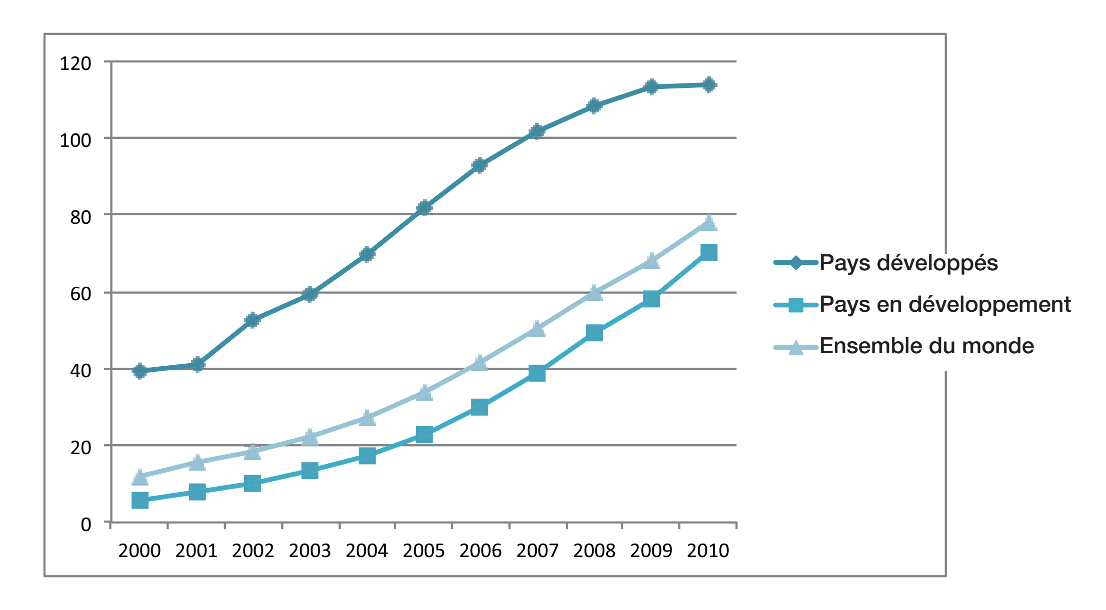


Figure 2[19] Nombre d'abonnements à la téléphonie mobile cellulaire pour 100 habitants, 2000-2010



16 Voir par exemple Sarrazin, T. (2011) Texting, Tweeting, Mobile Internet http://library.fes.de/pdf-files/bueros/africa-media/08343.pdf

17 ITU World Telecommunication 2010a. The World in 2010. Pg4. [en ligne] http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

18 ITU World Telecommunication, 2010. Pg16.

19 ITU World Telecommunication, 2010. Pg16.

La combinaison de l'Internet et de la téléphonie mobile a créé un environnement mondial des communications numériques qui évolue rapidement. Bien qu'une partie seulement des téléphones permettent d'accéder à l'Internet et qu'une partie encore plus réduite soient « intelligents », cela change rapidement et dans les cinq à dix années à venir, la plupart des observateurs pensent que l'accès à ces téléphones sera très répandu. Bien qu'il y ait eu des menaces sur la vie privée bien avant l'ère numérique, les défis actuels ont sensiblement changé à mesure que l'Internet a accru les capacités des gouvernements, des entreprises et des individus de s'immiscer dans la vie privée d'autrui. Beaucoup de commentateurs notent qu'une grande partie de la protection de la vie privée dont nous jouissions dans le passé était une protection par défaut – car les difficultés à surmonter pour surveiller les individus étaient trop complexes ou coûteuses, la technologie ne pouvait pas suivre et le personnel était insuffisant ou trop coûteux. Avec le développement de l'Internet et la disponibilité de communications numériques interactives efficientes, surveiller autrui est devenu plus facile, moins coûteux et plus efficient. L'Internet a considérablement augmenté l'impact sur les droits au respect de la vie privée des individus tant dans leur identité que dans le traitement de leurs données personnelles. L'utilisation de l'Internet et les transactions sur l'Internet génèrent une grande quantité d'informations personnelles qui sont centrales pour le modèle d'affaires des entreprises qui opèrent sur le réseau, et la façon dont elles sont comprises, sinon réglementées, dans un environnement transnational en mutation rapide est un défi majeur pour les responsables de l'élaboration des politiques.

En gros, l'Internet :

- Permet de collecter de nouveaux types d'informations personnelles.
- Facilite (et exige sur le plan économique) la collecte et la localisation des informations personnelles.
- Offre aux acteurs publics et privés de nouvelles capacités d'analyse des informations personnelles.
- Crée de nouvelles possibilités d'utilisation commerciale des données personnelles.
- Pose de nouveaux défis à la réglementation étant donné la nature transnationale de l'Internet.

Nous examinons plus en détail ci-après les implications de chacun de ces aspects.

1.1.1 Nouveaux types d'informations personnelles

Les progrès technologiques ont produit des outils de collecte et de compréhension de types d'information qui dans le passé auraient été impossibles ou impraticables. Par exemple, le rôle de l'ADN dans l'hérédité n'a été confirmé que dans les années 1950 mais aujourd'hui les progrès de la génétique permettent aux scientifiques d'extraire l'ADN d'une personne d'échantillons de plus en plus minuscules et d'en savoir de plus en plus sur un individu à partir de son ADN. Le stockage numérique de l'ADN est un énorme avantage dans les tentatives d'élucidation des crimes vu qu'il a permis de revisiter un certain nombre de cas de meurtres non résolus et a aussi conduit à libérer un certain nombre d'innocents condamnés pour des crimes qu'ils n'avaient pas commis. Cependant, la conservation de l'ADN a des implications importantes pour le respect de la

vie privée (entre autres) car l'ADN contient diverses informations personnelles sensibles, comme la prédisposition à certaines maladies.

Il y a des innovations importantes en biométrie, telles que la reconnaissance faciale, le scannage du doigt et de l'iris, qui sont des méthodes d'identification de plus en plus populaires. Ces dispositifs biométriques se prêtent à des utilisations très diverses – ils sont utilisés pour prévenir les fraudes que pourraient commettre les détaillants et les restaurateurs, pour identifier les électeurs lors des élections, pour passer les contrôles d'immigration (au lieu d'utiliser un passeport), pour tenir les états de présence sur les lieux de travail, ou pour accéder aux zones de haute sécurité. Bien que ces applications soient socialement très utiles, elles suscitent des préoccupations concernant le contrôle de ces données numériques, en particulier des questions de stockage et d'accès. Une controverse particulière a été suscitée par les scanners corporels utilisés dans les aéroports à la suite de tentatives terroristes de dissimulation de bombes dans les vêtements sur les avions. Beaucoup de voyageurs sont hostiles à l'utilisation de technologies qui pénètrent les vêtements et produisent ce qui est avant tout une image dénudée d'un individu qui est vue par d'autres. Beaucoup y voient une intrusion dans leur vie privée. Ces images peuvent révéler des informations intimement personnelles comme le fait qu'une personne a eu recours à la chirurgie esthétique ou porte une poche de colostomie mais en tout état de cause beaucoup de gens considèrent leurs vêtements comme un élément essentiel de leur intimité corporelle. Face à ces préoccupations il y a la sécurité des passagers, bien entendu, mais dans cette situation qui fluctue rapidement, il est difficile de préserver l'équilibre approprié.

1.1.2 Collecte et localisation des informations personnelles

Chaque ordinateur, téléphone mobile ou autre appareil connecté à l'Internet possède une adresse IP unique, c'est-à-dire un identificateur unique, ce qui veut dire qu'il est localisable. L'aptitude à localiser tout appareil crée de nouveaux problèmes importants pour le respect de la vie privée. Parmi les nombreux outils qui ont été créés pour suivre les internautes, deux exemples courants sont les cookies et les Web bugs. Les cookies sont de petits morceaux de texte que les navigateurs Web stockent sur l'ordinateur d'un internaute. Le cookie « enregistre » chaque fois que l'internaute accède au navigateur et peut servir à suivre les sessions, à stocker les sites préférés, à authentifier, etc. Les internautes peuvent décider d'accepter ou non les cookies en changeant le paramétrage de leur logiciel de navigation, mais certains sites deviennent ainsi inaccessibles. Les Web bugs sont généralement invisibles pour l'internaute (leur taille est généralement de 1x1 pixel) et ils sont incorporés dans les pages Web et les courriels. Lorsque la page/courriel contenant le Web bug est visionné(e), elle/il renvoie l'information au serveur (y compris l'adresse IP de l'usager, l'heure et la date auxquelles la page/courriel a été visionné(e) et le navigateur sur lequel elle/il a été visionné(e).

Une adresse IP peut être reliée à l'identité physique d'une personne par de nombreux moyens. Beaucoup de sites Web et de FAI ont mis en place des systèmes d'authentification qui impliquent la divulgation d'une identité (en particulier lors des transactions commerciales électroniques) ; beaucoup d'applications exigent un courriel personnel ou d'autres formes d'identification, les gouvernements peuvent obliger les internautes à enregistrer leur adresse IP, ou l'identité peut même parfois être déduite des actions d'une personne en ligne (voir ci-dessous).

Un aspect clé de l'Internet est son interactivité si on le compare aux « vieilles » technologies telles que la télévision, la radio et les téléphones. Les usagers doivent souvent fournir des informations sur eux-mêmes à chaque stade – par exemple quelles recherches ils font, sur quels liens ils cliquent, quelles pages ils consultent et combien de temps. Une série d'outils et de dispositifs technologiques sont conçus pour collecter ces informations (par exemple TiVo, Xbox360, Google Books)[20]. C'est un élément central du modèle économique de l'Internet. La numérisation de l'information et l'attente d'un libre accès rendent plus complexes les formes traditionnelles de génération de revenus sur l'Internet. Les entreprises qui réussissent exploitent donc délibérément les données personnelles pour cibler la publicité sur les internautes. Il y a donc une incitation économique directe et puissante à obtenir, conserver et partager les données personnelles. Cela s'applique aussi aux activités électroniques hors Internet. Les codes barres numérisés peuvent servir à suivre les achats des individus qui sont à leur tour utilisés pour contrôler le niveau des stocks et cibler les incitations ou le marketing sur ces consommateurs. Les cartes de transport numérisées telles que la carte London Oyster créent une image numérique de chaque trajet qui peut être utilisée pour suivre les mouvements des passagers dans la ville – ce qui est utile pour planifier les transports mais aussi pour suivre les déplacements d'un individu. Comme l'Internet est utilisé dans de plus en plus d'interactions quotidiennes dont les transactions bancaires, les achats commerciaux et la socialisation, les gens livrent de plus en plus de données personnelles, comprenant, souvent à leur insu, des informations sensibles sur leurs finances, leur santé et même leur sexualité. Ces innovations permettent de recueillir des informations toujours plus nombreuses et, comme l'a fait remarquer Lawrence Lessig, « votre vie devient une archive de plus en plus volumineuse »[21].

Il est aussi devenu beaucoup plus facile d'observer et de localiser les gens en ligne grâce à la surveillance électronique. Les caméras de télésurveillance et les satellites servent à surveiller les espaces publics et privés et ils sont à la disposition de plus en plus de gens. Les informations de localisation sont maintenant extraordinairement peu coûteuses grâce à des initiatives comme Google Earth. Les Systèmes de positionnement global (GPS) sont incorporés dans de plus en plus d'appareils vendus au public. Les étiquettes d'identification par radiofréquence (RFID) sont un autre exemple. Ces étiquettes étaient onéreuses, mais les prix chutent et en fin de compte elles pourraient servir à identifier non seulement le produit qu'achète un consommateur mais aussi avec quelle fréquence il est utilisé et où[22].

1.1.3 Nouvelles capacités des acteurs privés en matière d'analyse des informations personnelles

L'accroissement de la puissance des ordinateurs signifie que de vastes quantités d'informations, une fois collectées, peuvent être à peu de frais et de manière efficiente stockées, regroupées et analysées. Les progrès technologiques permettent de connecter entre elles les bases de données d'information, ce qui permet de traiter des volumes encore plus grands de données. Le risque de violations de la vie privée augmente de façon exponentielle quand on combine les technologies : par exemple en reliant les bases de

20 Privacy International, 2006.

21 Lessig, L. (1999) "Code and the Laws of Cyberspace" Basic Books, New York. Page 152.

22 Martínez-Cabrera, A. (2010) Privacy concerns grow with the use of RFID tags http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/09/05/BUCE1F8C1G.DTL

données sur la reconnaissance faciale (utilisées sur Facebook, par exemple) aux caméras de télésurveillance, il serait possible de suivre les individus plus que jamais auparavant.

La pratique consistant à fusionner et regrouper différentes bases de données informationnelles est très répandue. L'appariement de données provenant de sources différentes, par exemple des données fiscales et des données sur la santé ou des données financières et des données de sécurité sociale, soulève clairement des questions de respect de la vie privée. De plus, il est possible d'extraire des données personnelles des diverses techniques et ensuite de les apparier aux données publiques pour construire un profil personnel détaillé.

EPIC, organisme basé aux États-Unis qui s'occupe de respect de la vie privée, note que « les collecteurs d'informations sur les consommateurs sont enclins à catégoriser, compiler et vendre pratiquement n'importe quel élément d'information ». Par exemple, le Medical Marketing Service vend des listes de personnes qui souffrent de différentes pathologies. Ces listes sont croisées avec les informations concernant l'âge, le niveau d'instruction, la taille du logement de la famille, le sexe, le revenu, le style de vie, le statut matrimonial et la présence d'enfants. La liste des pathologies comprend le diabète, le cancer du sein et les cardiopathies. D'autres sociétés vendent des bases de données d'information sur les styles de vie des individus, leurs lectures et même leur religion[23].

Les bases de données combinées ont de multiples utilisations. Elles peuvent servir à l'exploration de données, qui est « le processus consistant à trouver des constantes dans les informations contenues dans les grandes bases de données »[24]. L'exploration des données se prête elle-même à de nombreuses utilisations, dont beaucoup sont bénéfiques comme par exemple lorsqu'il s'agit d'identifier des constantes indiquant une utilisation frauduleuse de cartes de crédit. Certains commentateurs affirment que l'exploration des données est neutre, mais elle peut avoir des implications pour la confidentialité. L'exploration des données ou leur fusion signifie souvent que l'on utilise des informations sur les personnes d'une manière qu'elles n'ont pas approuvée et dont elles ne sont même pas conscientes. De plus, le vaste ensemble de données utilisées comprend souvent des détails personnels et peut facilement être relié aux individus à leur insu.

Une autre utilisation courante est le profilage des données qui est l'utilisation de données agrégées pour « identifier, catégoriser et généralement prendre des décisions sur des individus que le décideur ne connaît que par leur profil numérisé »[25]. Les entreprises et les gouvernements peuvent utiliser le profilage des données pour établir des profils détaillés des individus. EPIC donne l'exemple d'une femme qui a poursuivi en justice la société Metromail basée aux États-Unis après qu'un de ses employés préposé à la saisie des données l'a harcelée sur la base d'informations qu'elle avait fournies lors d'une enquête. Durant le procès, il s'est avéré que Metromail détenait un dossier de 25 pages sur la femme, incluant « son revenu et ce qu'elle avait dit à propos de son utilisation de médicaments contre les hémorroïdes »[26].

---

23 Rotenburg M. et Hoofnagle C. "Submission to the House Government Reform Committee on Data Mining" 25 mars 2003. http://epic.org/privacy/profiling/datamining3.25.03.html

24 Fayyad, U., Grinstein, G. et Wierse, A. (2001) "Information Visualization in Data Mining and Knowledge Discovery". Morgan Kaufman Publishers.

25 Netter, W. "The Death of Privacy" Privacy Module I: Data Profiling Introduction, University of Harvard, 2002 http://cyber.law.harvard.edu/privacy/Module2_Intro.html

26 EPIC, "Privacy and Consumer Profiling" http://epic.org/privacy/profiling/

Pour protéger la confidentialité (et contourner les lois sur le respect de la vie privée), les sociétés désidentifient ou anonymisent souvent les données. Il s'agit d'un processus consistant à dépouiller les données des identificateurs personnels (tels que le nom, le numéro de sécurité sociale et l'adresse IP). Toutefois, des études révèlent qu'il est souvent possible de faire remonter des informations « anonymisées » à un individu. Par exemple, une étude réalisée en 1990 aux États-Unis d'Amérique a constaté que les données collectées lors d'un recensement (code postal, date de naissance et sexe) pouvaient être croisées pour identifier avec certitude 87% de la population du pays[27]. Un exemple plus récent remonte à 2006, lorsqu'AOL a publié des données sur les recherches des usagers qui étaient en principe non identifiables ; les chercheurs ont ensuite pu identifier de nombreux usagers grâce au phénomène assez habituel des recherches dans lesquelles l'usager saisit son propre nom[28].

Les bases de données peuvent être très difficiles à protéger, surtout lorsqu'on peut y accéder à distance et que l'accès est autorisé à beaucoup d'individus. Cela fait que les données personnelles des bases de données sont vulnérables à toutes sortes de cybercriminels. De plus, les informations sont souvent divulguées dans le domaine public. C'est souvent pour des motifs légitimes, mais cela peut susciter des préoccupations concernant la confidentialité. Par exemple, la base de données WHOIS contient des détails sur les contacts personnels de l'individu ou de l'organisation qui a enregistré chaque nom de domaine. Ces données sont publiques pour permettre aux administrateurs du réseau de résoudre facilement les problèmes sur l'Internet[29]. Un autre exemple est le mouvement lancé dans de nombreux pays pour publier les documents publics dans un format numérisé. Ces informations auraient été disponibles précédemment (telles que les certificats de naissance, de mariage et de décès) mais les nouveaux formats font qu'elles sont de plus en plus accessibles et faciles à croiser[30].

1.1.4 Nouvelles capacités des gouvernements en matière d'analyse des informations personnelles

Les gouvernements s'efforcent de mobiliser la puissance de l'Internet au service de leurs fonctions. Il y a eu une évolution spectaculaire vers la gouvernance électronique comme moyen de fournir des services à moindre coût et personnalisés. En conséquence, de nombreux pays tentent de rationaliser et de coordonner la fourniture des services en mettant en place de grandes bases de données contenant des informations personnelles sur les citoyens. Les cartes d'identité, par exemple, sont utilisées sous une forme ou une autre dans pratiquement tous les pays du monde, et les cartes nationales d'identité sont obligatoires dans une centaine de pays[31]. Les gouvernements s'orientent de plus en plus vers la saisie des données biométriques sur les cartes et le stockage de ces informations dans d'énormes bases de données utilisables pour certifier l'accès par exemple à la sécurité sociale, à la santé et aux voyages et en suivre l'utilisation.

---

27 Sweeney, L. "Strategies for De-Identifying Patient Data for Research" Carnegie Mellon University, Data Privacy Lab, 1998 http://www.ocri.ca/ehip/2005/presentations/Sweeney_bw.pdf Page 26.

28 Soghoian, C. (2007) "The Problem of Anonymous Vanity Searches" Indiana University Bloomington - School of Informatics. Publié enligne à l'adresse http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953673 Page 1.

29 EPIC "WHOIS" accessed 15/03/10, publié en ligne à l'adresse http://epic.org/privacy/whois/

30 Privacy International, 2006.

31 Privacy International, 1996, ID Card Frequently Asked Questions https://www.privacyinternational.org/article/id-card-frequently-asked-questions

Ces technologies jouent un rôle particulièrement important dans le domaine de la prévention et de la répression de la criminalité. Même avant la « guerre contre la terreur », nombre de gouvernements utilisaient intensivement des technologies telles que la télésurveillance pour ces raisons. Depuis le 11 septembre, la menace terroriste a impulsé dans beaucoup de pays une utilisation plus intensive des mécanismes de surveillance, souvent selon des modalités qui sont intrusives et même violent les lois existantes sur la protection de la vie privée. Un exemple particulièrement pertinent est celui des voyages par avion. Comme indiqué précédemment, des scanners corporels sont utilisés ou testés aux États-Unis d'Amérique, au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, en Inde, en Australie, au Japon, dans la Fédération de Russie et aux Pays-Bas, entre autres[32]. Une autre pratique est l'utilisation de listes secrètes de personnes à surveiller, par exemple au Canada et aux États-Unis d'Amérique[33]. Les données personnelles sont soumises par les voyageurs en tant que condition à remplir pour voyager et ces informations sont vérifiées à partir de bases de données de provenance incertaine. Le profilage des données est utilisé pour créer une liste de personnes qui sont jugées constituer des menaces pour la sécurité, la liste est communiquée à d'autres pays et les personnes qui y figurent sont empêchées de prendre l'avion ou sont assujetties à des mesures de sécurité renforcées. Les listes de personnes à surveiller deviennent parfois publiques ; cela a mis en évidence des erreurs, mais stigmatisé des individus ; dans d'autres cas elles sont restées secrètes, ce qui veut dire que des individus se sont vu refuser un visa sans nécessairement avoir été déclarés coupables de quoi que ce soit ou avoir eu la possibilité de se défendre[34]. Dans une affaire célèbre au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, un musulman très connu, Yusuf Islam (précédemment le chanteur Cat Stevens) a été empêché de se rendre aux États-Unis d'Amérique (son vol United Airlines de Londres au Dulles International Airport de Washington a été dérouté sur Bangor, Maine, lorsque les agents des États-Unis examinant la liste des passagers ont découvert qu'il était à bord). Il y aurait eu des motifs liés à des connexions terroristes mais ces motifs n'ont jamais été explicités, bien que Yusuf Islam soit connu comme un musulman qui promouvait la paix et la réconciliation entre les communautés. L'interdiction a été levée par la suite.

Certains gouvernements ont pu utiliser ces technologies pour suivre beaucoup plus intensivement les actions de leurs citoyens, en particulier des dissidents. Par exemple, l'Initiative OpenNet indique qu'en Chine, le système de messagerie instantanée en ligne le plus populaire (QQ) enregistre les communications des usagers en ligne et en rend compte à la police. En 2006, le Ministère chinois de la sécurité publique a annoncé le lancement du projet « Bouclier d'or », destiné à devenir un système national de surveillance numérique. En 2008, une société publique de téléphonie mobile a révélé qu'elle avait un accès illimité aux données des consommateurs et qu'elle les transmet au Gouvernement chinois sur demande. L'exemple le plus flagrant a été en 2009 la tentative du Gouvernement chinois visant à faire en sorte que le logiciel connu sous le

---

32 Cavoukian, A. "Whole Body Imaging in Airport Scanners: Building in Privacy by Design" Information & Privacy Commissioner, Ontario, Canada. Juin 2009 http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf Page 2.

33 Conseil des droits de l'homme, treizième session, point 3 de l'ordre du jour. 28 décembre 2009, A/HRC/13/37 http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf Page 17.

34 Ibid.

nom de Barrage vert soit intégré dans tous les ordinateurs personnels vendus en Chine[35]. Ce logiciel aurait suivi les comportements individuels des internautes en installant des composants dans le système d'exploitation et aurait donné aux autorités le pouvoir de contrôler directement l'accès aux contenus (et aussi permis un contrôle à distance de l'ordinateur utilisant le logiciel)[36]. La proposition a finalement été écartée par l'OMC pour des motifs commerciaux. Plus récemment, les autorités chinoises auraient tenté de faire installer par les cafés, les hôtels et autres commerces du centre de Beijing des technologies de surveillance des usagers du Wifi, ce qui a été considéré comme un autre exemple de renforcement des contrôles de l'utilisation de l'Internet[37].

Le Rapporteur spécial sur la lutte antiterroriste et les droits de l'homme a noté des exemples de pratiques de surveillance en Allemagne, en Colombie, au Bangladesh et aux États-Unis d'Amérique qui ont suscité sa préoccupation[38]. Une étude de Privacy International de 2007 a révélé une dégradation globale des protections et sauvegardes de la vie privée, ainsi qu'une augmentation des cas de surveillance dans 47 pays.

La cybercriminalité est un problème croissant sur l'Internet, avec des estimations évaluant le coût des vols en ligne à 1 billion de dollars des États-Unis[39]. Les mesures de sécurité insuffisamment sévères et les atteintes à la sécurité peuvent avoir pour résultat que des criminels volent les données d'autres personnes qui peuvent ensuite être utilisées pour commettre de nombreuses infractions telles que la fraude, le vol ou le harcèlement.

Enfin, les technologies de surveillance sont utilisées beaucoup plus localement, pour surveiller le comportement des membres de la famille et des employés. Au lieu de surveiller les employés qui ont des comportements suspects, il apparaissait que de nombreux employeurs instituaient une surveillance systématique continue sur le lieu de travail[40]. De fait, il y a maintenant un marché pour les nouvelles technologies capables de détecter des comportements complexes des employés et de rendre compte à l'employeur – l'appareil peut différencier entre des actions telles que « frotter, balayer, marcher et même vider une poubelle »[41].

1.1.5 Nouvelles possibilités commerciales d'utilisation commerciale des données personnelles

L'Internet a généré un volume considérable d'activité économique. Une étude récente de McKinsey estime que les effets économiques directs et indirects de l'Internet représentent

---

35 Opennet Initiative, China's Green Dam: The Implications of Government Control Encroaching on the Home PC http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

36 Wolchok, S., Yao, R. et Halderman, A. (2009) Analysis of the Green Dam Censorware System http://www.cse.umich.edu/~jhalderm/pub/gd/

37 Branagan, T. (2011) China boosts Internet surveillance http://www.guardian.co.uk/world/2011/jul/26/china-boosts-Internet-surveillance

38 Conseil des droits de l'homme, 2009, p. 14, 15.

39 Weber, T. Cybercrime threat rising sharply, BBC News, 31/01/09 http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

40 Bonsor, K. Is your workplace tracking your computer activities? http://computer.howstuffworks.com/workplace-surveillance1.htm

41 Fitzpatrick, M. "Mobile that allows bosses to snoop on staff developed" BBC News 10/03/2010 http://news.bbc.co.uk/1/hi/technology/8559683.stm

3,4 % du PIB dans les 13 pays étudiés mais 21% de la croissance économique dans les cinq économies matures, avec 2,6 emplois créés pour un perdu[42].

Les entreprises de l'Internet telles que Google, Yahoo et Facebook ont accès à une quantité astronomique de données[43]. Les plus grosses ont d'énormes bases d'usagers (par exemple, Facebook a plus de 800 millions d'usagers[44]) et cherchent à couvrir de plus en plus d'interactions (par exemple un usager peut se servir de Google pour localiser des informations en ligne, envoyer des courriels, visionner des vidéos, acheter des produits, etc.). Nombre des services fournis par ces entreprises sont gratuits et leurs modèles d'affaires reposent sur la collecte d'informations sur les usagers et leur utilisation à des fins de marketing. Les données sur les usagers ont donc une grande valeur économique. Une étude de 1999 a découvert que 92 % des sites Web recueillaient au moins un type d'information permettant d'identifier leurs usagers (par exemple leur nom, leur adresse électronique et leur adresse postale)[45] et on peut penser que depuis lors la collecte d'informations n'a fait qu'augmenter. Les entreprises ont aussi tendance à observer le plus grand secret quant aux informations qu'elles recueillent et comment ; comme l'a noté The Economist, cette attitude s'explique autant par la volonté de préserver leur compétitivité que par des considérations tenant à la vie privée[46].

Une grande partie de cette activité économique dépend des intermédiaires de l'Internet – les divers acteurs, services et applications qui facilitent les transactions entre les tiers sur l'Internet, y compris par exemple les moteurs de recherche et les FAI. Les communications fondées sur l'Internet reposent de plus en plus sur ces intermédiaires pour accéder, traiter et transmettre les données. Le pouvoir croissant des intermédiaires et leur contrôle sur les données personnelles ont suscité un certain nombre de préoccupations quant à la question de savoir si les réglementations en vigueur sont suffisantes pour protéger les droits au respect de la vie privée. Trois types d'intermédiaires suscitent des préoccupations particulières – les sites des réseaux sociaux, les capacités de l'informatique en nuage et les moteurs de recherche.

Sites des réseaux sociaux

Les sites des réseaux sociaux sont des sites Web centrés sur l'établissement et/ou le reflet de relations sociales entre les personnes. Certains facilitent des « amitiés » virtuelles avec des personnes qui sont déjà connues de l'usager hors ligne, leur permettant d'échanger des photos et de converser en ligne. D'autres s'attachent à permettre aux gens de se faire de nouveaux amis, souvent avec un ciblage particulier tel que les relations de travail (LinkedIn) ou les goûts musicaux (Pandora). Chaque service est différent, mais le format standard permet aux usagers de créer leur propre page Web contenant diverses

---

42 McKinsey Global Institute, (2011) Internet matters: The Net's sweeping impact on growth, jobs, and prosperity http://www.eg8forum.com/fr/documents/actualites/McKinsey_and_Company-internet_matters.pdf

43 Massimino, E. (2012) Privacy, Free Expression And The Facebook Standard http://www.forbes.com/sites/realspin/2012/01/31/privacy-free-expression-and-the-facebook-standard/

44 Protalanski, E. (2012) Facebook has over 845 million users https://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332

45 Federal Trade Commission, (1999) "Self-regulation and Privacy Online: A Report to Congress" Mars 1999, publié en ligne à l'adresse http://www.ftc.gov/os/1999/07/privacy99.pdf Page 4.

46 Economist, (2010) "Clicking for Gold: How internet companies profit from data on the Web", in "A special report on managing information" The Economist, Volume 394, Number 8671.

informations personnelles (date de naissance, lieu de résidence, intérêts, nom). Les usagers peuvent ensuite se relier à des amis qui pourront voir leurs informations et vice-versa. Les sites des réseaux sociaux sont très populaires, avec des centaines de millions d'usagers au total. Toutefois, les violations de la vie privée causées par ces sites ont suscité des préoccupations croissantes. Certaines préoccupations ont trait à la maîtrise des communications et des médias, car beaucoup d'usagers n'ont pas conscience des risques qu'implique la divulgation d'informations personnelles à autrui. Beaucoup ne prennent pas de précautions s'agissant des personnes auxquelles ils permettent de voir leurs données, et il semble que beaucoup prennent pour amis des gens qu'ils ne connaissent pas bien. Cela peut avoir des conséquences considérables étant donné par exemple que sur Facebook l'usager moyen a 130 amis sur le site[47]. Cela sera examiné plus en détail dans la section suivante.

Informatique en nuage

L'informatique en nuage est une nouvelle architecture des réseaux dans laquelle les données, la puissance de traitement ou les logiciels sont stockés sur des serveurs éloignés, par opposition à l'ordinateur personnel, et rendus accessibles via l'Internet. Il existe différentes formes d'informatique en nuage qui fournissent une série de services. Les particuliers ou les organisations peuvent en fait louer de la capacité de calcul à des fournisseurs de services éloignés. Par exemple, le service Apps de Google permet aux gens de créer et de sauvegarder des feuilles de calcul et des documents sur traitement de texte en ligne. Les autres services comprennent les plates-formes collaboratives qui permettent aux usagers d'accéder simultanément à des documents, tels que les plates-formes wiki et Google docs[48].

L'informatique en nuage peut produire plusieurs résultats positifs. Elle peut par exemple réduire le coût d'achat et de mise à jour des logiciels pour les petites entreprises et organisations, ce qui peut être particulièrement utile aux usagers aux ressources financières limitées dans les pays en développement. Elle peut aussi améliorer le confort des usagers en leur permettant d'accéder à des documents partout dans le monde et d'écrire des documents en collaboration avec des coauteurs travaillant dans d'autres régions géographiques.

Cependant, l'informatique en nuage suscite aussi un certain nombre de préoccupations du point de vue de la confidentialité. Comme les données sont stockées sur un logiciel d'un tiers, la responsabilité de la protection de ces informations incombe au tiers et les usagers perdent un certain contrôle. De plus, les lois applicables à l'informatique en nuage ne sont pas bien définies, de sorte que les usagers ne sont pas sûrs de la confidentialité de leurs données. Les termes et conditions (T&C) d'utilisation prévoient parfois que le prestataire de services peut fermer des comptes ou supprimer/éditer des contenus à sa discrétion. C'est le cas par exemple de Mozy.com, service qui permet aux usagers de sauvegarder les informations stockées sur leur PC en ligne[49]. Il y a un danger que les usagers perdent leurs informations personnelles. Beaucoup de T&C limitent strictement la responsabilité du prestataire de services, ce qui pourrait signifier qu'au cas où la

47 Facebook, (2012) " Statistics" publié en ligne à l'adresse http://www.facebook.com/press/info.php?statistics

48 EPIC "Cloud Computing" publié en ligne à l'adresse http://epic.org/privacy/cloudcomputing/

49 Ibid.

sécurité serait prise en défaut et où les usagers perdraient leurs données personnelles, ceux-ci risqueraient de n'avoir droit à aucune indemnisation. Enfin, il est fréquent que les fournisseurs de services ne mentionnent pas le sort des informations d'un usager une fois qu'ils ont fermé ou supprimé le compte. Cela ne signifie pas toujours que les informations sont supprimées, ce qui pourrait entraîner des atteintes à la confidentialité[50]. Les implications de l'informatique en nuage pour la confidentialité sont examinées plus en détail dans la section suivante.

Moteurs de recherche

Les moteurs de recherche jouent un rôle crucial en tant qu'intermédiaires sur l'Internet, permettant aux individus de trouver des contenus et d'y accéder. Ce sont par exemple Google, Bing, Ask.com et Yahoo! Search. Les moteurs de recherche collectent généralement quantité de données personnelles, dont les adresses IP, les recherches, ainsi que l'heure, la date et l'emplacement de l'ordinateur soumettant la recherche. Comme indiqué précédemment, ces informations peuvent être personnellement identifiables et peuvent révéler des éléments particulièrement sensibles tels que les convictions politiques d'une personne, son orientation sexuelle, ses croyances religieuses et des renseignements médicaux. Ces informations sont généralement utilisées à des fins de marketing, mais il y a aussi des risques de divulgation publique des informations, comme dans le cas de la publication d'informations par AOL en 2006 (évoquée ci-dessus). Les risques concernant le respect de la vie privée et les autres droits de l'homme sont d'autant plus grands dans les pays où la protection des droits de l'homme est limitée. Ces points sont examinés plus en détail dans la section suivante.

50 Ibid.

2. APERÇU MONDIAL DES DÉFIS ET DES OPPORTUNITÉS POUR LA PROTECTION DE LA VIE PRIVÉE SUR L'INTERNET

2.1 Questions clés

2.1.1 Défis et opportunités du maintien du contrôle sur les données personnelles en ligne

> « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. » – Article 12 de la Déclaration universelle des droits de l'homme.

La protection de la vie privée est depuis longtemps consacrée comme un droit fondamental de la personne humaine. Toutefois, avec les progrès techniques des dernières décennies, ce droit a été de plus en plus remis en question. Face à ces difficultés, il y a eu depuis les années 1980 une vague de lois sur la protection des données dans différentes régions du monde, qui ont tenté de sauvegarder les données personnelles des individus, mais la législation et la politique publique ont beaucoup de mal à suivre les cycles de plus en plus courts du développement des technologies. C'est sur l'Internet que ce problème est devenu le plus évident, et il est très douteux que l'affirmation de l'Union européenne selon laquelle « Toute personne a droit à la protection des données à caractère personnel la concernant »[51] soit respectée. Les usagers individuels de l'Internet contrôlent-ils leurs propres données personnelles, y compris les modalités de leur collecte, de leur conservation, de leur traitement et de leur divulgation ?

Dans la pratique, de nombreux attributs de l'Internet se révèlent très problématiques du point de vue du contrôle des utilisateurs sur leurs données personnelles. Le caractère transnational de l'Internet fait qu'il est difficile et parfois impossible de juger dans quels pays, juridictions et régions les données sont transmises. La vitesse et la portée des communications sur l'Internet sont si grandes que les données peuvent se disperser loin du contrôle effectif d'un individu en moins d'une seconde. De plus, il existe un marché substantiel sur l'Internet pour les données personnelles, impulsé par les modèles d'affaires fondés sur la publicité dans lesquels les usagers paient avec leurs données au lieu d'effectuer des paiements monétaires. D'autre part, le coût de ces données est extraordinairement bas, ce qui permet d'échanger des dizaines de milliers de données gratuitement ou presque. Les progrès des technologies de traitement

---

51 Article 8.1 de la Charte des droits fondamentaux de l'Union européenne, 2000.

informatisé permettent de traiter des volumes croissants de données personnelles. Les multiples parties associées à l'affichage d'une page de l'Internet sur l'écran d'un usager compliquent considérablement ce processus. La convergence croissante des appareils connectés à l'Internet fait aussi qu'il est particulièrement difficile de conserver le contrôle de ses données personnelles. Enfin, beaucoup d'internautes ont pris l'habitude de cliquer sur « Accepter » et de consentir à fournir leurs données sans prendre un tant soit peu de temps pour lire les conditions du service ou la politique du site concerné en matière de confidentialité.

La tension entre les droits et la capacité réelle de contrôle des internautes sur leurs données personnelles a conduit à de vastes débats sur la confidentialité sur l'Internet. Ces débats sont généralement centrés sur le défaut de contrôle et de pouvoir des internautes pour influencer les modalités d'utilisation et de traitement de leurs données, tout en soulignant le rôle des entreprises dans le contrôle et la gestion des données privées. De plus, le contrôle des acteurs privés est souvent contrasté avec celui des autorités publiques, considérées comme incapables ou peu désireuses de mettre en œuvre des protections réelles des données personnelles des internautes.

Ces débats peuvent être compris dans le contexte de plusieurs questions fondamentales. D'abord et avant tout, la question du consentement éclairé des usagers et comment il peut être obtenu, garanti ou même révoqué. Deuxièmement, la question de la transparence et de la « lisibilité » des politiques de confidentialité pour les usagers. Troisièmement, l'aptitude des usagers, des acteurs privés et des entités publiques à mettre en œuvre efficacement leurs choix individuels concernant l'utilisation des données personnelles sur l'Internet. Même si la plupart des usagers, des acteurs privés et des entités publiques sont d'accord, la diffusion des données personnelles est telle qu'elle peut rapidement échapper au contrôle de tout acteur (voir l'encadré ci-dessous pour plus de détails).

Quatrièmement, les droits des internautes de contrôler leurs données personnelles peuvent entrer en conflit avec d'autres droits, tels que le droit d'autrui à la liberté d'expression. Comme il est dit dans l'encadré ci-dessous sur l'intimité visuelle et Edison Chen, les conflits sont fréquents entre les reportages des médias sur les personnages publics et leur droit de contrôler leurs données personnelles. Cinquièmement, le rôle problématique de la surveillance de l'Internet par les autorités publiques reste difficile. Enfin, le caractère approprié de l'anonymat ou de l'usage de pseudonymes en ligne représente un élément important du débat général sur la protection de la vie privée sur l'Internet. Toutes ces questions sont intimement liées à la confidentialité de l'information, mais elles apportent aussi une réponse au défi plus général : quel Internet espérons-nous créer ? Quel que soit le groupe de parties prenantes, l'État nation ou l'ensemble d'acteurs que puisse représenter ce « nous », envisager une vision commune d'un futur Internet peut aider à comprendre comment y parvenir. Donner des réponses de fond à cette question façonnera fondamentalement l'Internet mondial dans sa totalité.

I) L'intimité visuelle et Edison Chen

Edison Koon-Hei Chen était un des acteurs les plus connus de Hong Kong. Il jouait dans de nombreux films régionaux et internationaux et était considéré comme un des acteurs majeurs de la région, jouant aussi dans des productions

de Hollywood telles que The Dark Night. En janvier 2008, des images sexuelles de Chen avec d'autres femmes de l'industrie cinématographique chinoise ont commencé à apparaître sur l'Internet et ont été largement diffusées dans les médias grand public. Bien que les autorités de police nationales et internationales aient participé aux efforts visant à enrayer la diffusion de ces images, elles ont semble-t-il échoué[52]. Les images ont continué de se répandre sur l'Internet et en conséquence le nom de l'acteur est devenu un des plus recherchés sur l'Internet en Chine en 2008[53]. Un technicien qui réparait l'ordinateur portable d'Edison Chen a finalement été condamné pour avoir volé les images lors de cette réparation en 2007[54]. Une fois les images en ligne, il était extrêmement difficile sinon impossible de les supprimer. Dans ce contexte, la demande publique massive de ces images a garanti leur large diffusion. La large republication des images et la demande correspondante violaient clairement la vie privée, et la demande publique massive de telles images soulève des questions quant aux moyens de promouvoir une culture de la confidentialité de l'information.

2.1.2 Initiatives visant à protéger la confidentialité et l'anonymat en ligne

Pour répondre à beaucoup de ces questions, diverses initiatives ont été lancées sur l'Internet afin de protéger la vie privée des individus. À ce propos, il est extraordinairement important que la société civile initie et organise des initiatives visant à protéger la confidentialité et l'anonymat en ligne.

Ce rôle est reflété dans les nombreuses initiatives importantes conduites par la société civile. Dans ce contexte, une des initiatives majeures a consisté à élever le niveau de sensibilisation et d'éducation des usagers quant à l'importance du respect de leur vie privée et des moyens de la protéger. Les exemples notables incluent le projet « Surveillance Self Defence » créé par l'Electronic Frontier Foundation (EFF), « Big Brother Inc. », projet profilant les entreprises exportant des technologies de surveillance, et « Me and my own Shadow », campagne de sensibilisation menée par l'ONG TacticalTech.

II) Initiatives citoyennes sur la conservation des données

Une des initiatives les plus remarquables des usagers en faveur de la protection de la confidentialité et de l'anonymat sur l'Internet est l'initiative citoyenne allemande sur la conservation des données. Plus de 34 000 citoyens ont lancé en 2007 une plainte de masse auprès de la Cour constitutionnelle allemande de masse contre

52 Pang, D., Chen, B., et Lee, D. (2008). Eight now held in internet sex probe. The Standard. Extrait le 13 décembre 2011 de http://www.thestandard.com.hk/news_detail.asp?pp_cat=12&art_id=61125&sid=17431562&con_type=3#

53 Google. (2008). Google Zeitgeist 2008. Extrait le 13 décembre 2011de https://www.google.com/intl/en/press/zeitgeist2008/world.html#top

54 Pomfret, J. (2009). Technician guilty in Edison Chen sex pictures trial. Victoria News. Extrait le 13 décembre 2011de http://www.vicnews.com/entertainment/television/43998412.html

la nouvelle loi allemande sur la conservation des données[55]. Ce recours collectif est le plus important jamais soumis à la Cour constitutionnelle allemande. Les avocats concernés ont mis plusieurs mois à traiter les signatures et à les soumettre à la Cour. Celle-ci a d'abord émis en 2008 une injonction préliminaire contre la nouvelle loi sur la conservation des données et a finalement déclaré la loi inconstitutionnelle en 2010[56]. Comme très peu même des recours constitutionnels sont déclarés admissibles par la Cour et que 1 à 2 % seulement aboutissent à un résultat positif, le succès de ce recours a été un moment historique. En tant que telle, l'initiative a été un succès car non seulement elle a abouti à la déclaration d'inconstitutionnalité de la loi allemande sur la conservation des données, mais elle a aussi amené la confidentialité et l'anonymat au premier plan du débat public en Allemagne. Comme la loi allemande sur la conservation des données transposait une directive de l'UE dans le droit allemand, les conséquences de cette décision se sont fait ressentir bien au-delà des frontières de l'Allemagne et ont fortement influencé le débat et la pratique de la conservation des données en Europe.

Chacun de ces projets démontre l'importance du rôle joué par la société civile dans la sensibilisation aux questions de respect de la vie privée, fournissant aux internautes des ressources pour défendre leur vie privée et informer les citoyens sur les agissements de l'industrie de la surveillance. Les organisations, tant internationales que nationales, de la société civile, ont joué un rôle crucial dans ce contexte en donnant aux utilisateurs de la technologie les moyens de faire des choix éclairés au sujet de leurs données personnelles.

Les initiatives techniques jouent aussi un rôle utile dans la protection de la confidentialité et de l'anonymat en ligne. La mise au point d'outils en libre accès à l'intention des internautes tels que Tor, GnuPG ou HTTPSEverywhere ont contribué substantiellement à la confidentialité et à l'anonymat des internautes. Ces programmes en accès libre offrent aux internautes un niveau plus élevé d'anonymat lorsqu'ils utilisent l'Internet, leur permettent de sécuriser leurs fichiers et leurs courriels ou leur offrent une plus grande sécurité lorsqu'ils accèdent à de nombreux sites Web.

Tous ces efforts techniques ont bénéficié d'un large soutien et concours des internautes à travers le monde et de diverses organisations de la société civile. Il est à noter que la plupart des initiatives du secteur privé sont axées sur l'offre aux utilisateurs finals de puissantes technologies de cryptage, contrepoids inestimable aux techniques de surveillance de l'Internet. Il a été estimé à maintes reprises par les universitaires, les experts techniques et la société civile qu'un développement substantiel de l'utilisation de puissantes techniques de cryptage par les internautes aurait un impact très positif sur la confidentialité et l'anonymat sur l'Internet.

---

55 Initiative Vorratsdatenspeicherung. (2011). Stoppt die Vorratsdatenspeicherung. Extrait le 13 décembre 2011 de https://www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html

56 BVerfG, 1 BvR 256/08, le 2.3.2010, Paragraphe (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

III) Initiatives entrepreneuriales de promotion de la liberté d'expression et de la confidentialité : l'Initiative mondiale des réseaux (Global Network Initiative)

En dehors des initiatives citoyennes, une des plus notables initiatives d'autorégulation des entreprises de l'Internet est l'Initiative mondiale des réseaux (Global Network Initiative - GNI). Cette initiative rassemble plusieurs entreprises de technologie, ONG et universitaires. Si elle a été une réussite en matière de sensibilisation au rôle des entreprises dans la protection et la promotion des droits au respect de la vie privée et à la liberté d'expression, le nombre des entreprises membres de la GNI reste limité, avec seulement quelques grandes entreprises participantes : Google, Yahoo et Microsoft.

Bien que beaucoup d'autres entreprises de l'Internet aient été invitées à rejoindre la GNI, ces appels sont presque tous restés sans écho. Comme la GNI est relativement jeune, il reste à voir comment ses exigences en matière d'information auront une incidence sur les pratiques effectives des entreprises à moyen et à long terme.

À côté des initiatives de la société civile, les initiatives des internautes ont aussi joué un rôle important dans la sauvegarde de la confidentialité et de l'anonymat en ligne. Ces initiatives tendent à cibler une question spécifique plutôt que le concept de confidentialité dans son ensemble. Les campagnes en faveur de changements des « politiques du nom réel » sur l'Internet et de sensibilisation au danger de la communication de données personnelles sur l'Internet, ainsi qu'une pétition de plus de 30 000 internautes adressée à la Cour suprême allemande pour contester la constitutionnalité des lois sur la conservation des données, sont des exemples notables d'initiatives importantes des usagers visant à protéger la confidentialité et l'anonymat en ligne.

Il faut aussi mentionner les initiatives entrepreneuriales visant à protéger la confidentialité, dont la Global Network Initiative est une des plus connues (voir encadré ci-dessus). Toutefois, l'efficacité de l'autorégulation des entreprises sur l'Internet suscite de larges débats. Surtout ce qui concerne la confidentialité, il est fréquemment soutenu que les entreprises profitent de la vente des données de leurs consommateurs et qu'elles n'ont pas intérêt à offrir autre chose que des projets « feuille de vigne » de responsabilité sociale des entreprises destinés à masquer leurs motivations réelles. La réponse la plus fréquente à cette assertion est que les sociétés ont besoin de la confiance des usagers et que toute atteinte substantielle à cette confiance serait néfaste à la société qui s'en rendrait coupable. Quoi qu'il en soit, il y a clairement des motivations contradictoires pour les entreprises qui s'engagent dans de telles initiatives et il est très douteux que les systèmes d'autorégulation en matière de confidentialité puissent remplacer dans une large mesure les lois et réglementations publiques.

Enfin, il y a chez nombre de défenseurs de la confidentialité et de l'anonymat un notable scepticisme quant à l'efficacité des solutions réglementaires, judiciaires ou gouvernementales. Il y a une crainte largement répandue que la réglementation publique de la confidentialité ne soit contreproductive, accaparée par les intérêts particuliers, mal

informée ou au mieux inefficace. Alors que les défenseurs ont constamment demandé que l'on change les réglementations relatives à la confidentialité et continuent à chercher à obtenir réparation des violations de la confidentialité en s'adressant aux tribunaux, l'accent est par ailleurs fortement mis sur l'autonomisation des usagers pour faire en sorte qu'ils ne soient pas dépendants des réglementations publiques. Cette approche est axée sur la fourniture aux usagers des outils dont ils ont besoin pour protéger leur propre vie privée et sur la sensibilisation aux questions de confidentialité. La stratégie principale d'autonomisation des usagers finals pour qu'ils protègent leur vie privée donne à penser que nombre de défenseurs ne sont pas convaincus que les États sont capables ou désireux de s'attaquer à certains des problèmes les plus épineux touchant la confidentialité.

2.1.3 Les rôles et responsabilités des fournisseurs d'accès et des intermédiaires

Les fournisseurs d'accès à l'Internet et les intermédiaires de l'Internet ont un rôle particulièrement important à jouer sur l'Internet. Ce rôle s'étend bien au-delà du rôle habituel d'une entreprise qui fournit un produit standard dans un marché ordinaire. Parce que les fournisseurs d'accès à l'Internet et les intermédiaires de l'Internet s'occupent d'information, ces entreprises sont capables, par leurs actions, de sauvegarder ou de détruire beaucoup des droits et des libertés des usagers sur l'Internet. De plus, leur rôle ne se situe pas dans un vide de pouvoir et différents dispositifs nationaux et internationaux de gouvernance et intérêts politiques et commerciaux sont souvent en concurrence pour renforcer le contrôle sur les intermédiaires de l'Internet. En conséquence, protéger ces entreprises contre la « responsabilité des intermédiaires » ne va pas de soi mais représente un compromis politique spécifique qui est constamment contesté dans de nombreux contextes différents[57]. En réponse à ces exigences, les défenseurs des droits de l'homme ont avancé des arguments solides pour demander l'élaboration de règles régissant la responsabilité des intermédiaires conformément aux normes des protections internationales[58].

Toutefois, dans de nombreux cas, il y a d'autres mécanismes par lesquels les intermédiaires sont contraints de violer la confidentialité de leurs usagers que la simple responsabilité juridique. Les fournisseurs d'accès à l'Internet (FAI), en particulier, sont fréquemment contraints de « contrôler volontairement » les actes de leurs usagers, ce qui a pour effet de créer des infrastructures et des institutions qui collectent et manipulent les données personnelles des usagers dans des proportions qui vont bien au-delà des besoins des mécanismes nécessaires uniquement pour fournir les services de l'Internet. C'est là seulement un des multiples exemples de situations dans lesquelles les intermédiaires sont contraints ou persuadés de satisfaire aux désirs de tiers de violer et de restreindre la confidentialité de leurs usagers.

D'autre part, plus ces intermédiaires de l'Internet sont transnationaux et déconnectés de tout emplacement physique dans leurs opérations, plus de souplesse ils obtiennent dans leurs transactions avec les autorités législatives concernées. Dans ce contexte,

---

57 Mueller (2010) Networks and States, Mueller, M. L. (2010). Networks and States: The Global Politics of Internet Governance, p. 138-139. MIT Press.

58 La Rue, F. (2011). Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, au Conseil des droits de l'homme de l'ONU (A/HRC/14/23) ; Genève, Organisation des Nations Unies.

un rôle particulier est joué par les grands intermédiaires transnationaux comme Google, Microsoft, Facebook ou Amazon qui peuvent négocier avec les États-nations d'égal à égal, semble-t-il, en raison de leur taille et de leur portée internationale. Le fait qu'ils vendent essentiellement des logiciels ou des services en ligne leur autorise un niveau considérable de flexibilité en ce qui concerne leur implantation physique. Le résultat est une aptitude à choisir les juridictions qui leur conviennent.

Les États-nations à travers le monde sont en concurrence pour accueillir les entreprises et toutes les indications du processus de recherche montrent que beaucoup de pays ont choisi, par stratégie, une réglementation peu contraignante de la protection de la vie privée. Il s'agit d'obtenir ainsi un avantage compétitif (présumé) par rapport aux autres économies développées. Dans bien des cas, ces choix stratégiques sont opérés par de petits pays qui ont décidé de devenir des plaques tournantes régionales pour les industries de haute technologie. La compétition semble confirmer que la concurrence des politiques de confidentialité entre les pays est au moins indirectement favorisée par les entreprises transnationales.

Un autre domaine qui est devenu extrêmement sujet à controverse du point de vue du respect de la vie privée est la législation sur la conservation des données. En vertu de cette législation, les fournisseurs d'accès à l'Internet sont associés à la surveillance et au stockage à grande échelle des pratiques privées de leurs clients sur l'Internet. Ces mesures sont généralement appliquées sur une grande échelle sans que l'on estime que les clients des FAI qui sont observés ont commis une infraction. Toutefois, il est souvent soutenu que ces mesures pourraient néanmoins aider à enquêter sur les infractions commises sur l'Internet. La protection des enfants (voir l'encadré pour plus de détails) et l'application du droit d'auteur sont d'autres domaines dans lesquels les fournisseurs d'accès à l'Internet et les intermédiaires de l'Internet ont été soumis à de fortes pressions pour qu'ils s'immiscent dans la vie privée de leurs clients[59] selon des modalités qui ne respectent pas les principes de la protection tels que la transparence, une procédure équitable et l'obligation redditionnelle.

La pression exercée sur des intermédiaires de l'Internet comme Google, Facebook ou Amazon peut aussi avoir des effets négatifs considérables sur la confidentialité de l'Internet. Contrairement aux interactions hors ligne, dans lesquelles il est extrêmement difficile de voir des interactions personnelles, économiques ou politiques sur une grande échelle, les interactions en ligne laissent une « trace de données ». Google a commencé à réagir à cette pression en publiant régulièrement des « rapports de transparence » pour informer les internautes sur la portée des données que lui demandent les gouvernements. C'est un premier pas utile, mais cela ne suffit pas à cartographier nombre des interactions coercitives informelles qui visent à obtenir des sociétés privées des données confidentielles ou à spécifier plus précisément pourquoi ces demandes ont été formulées.

Les fournisseurs d'accès à l'Internet (FAI) appartenant à l'État jouent un rôle particulièrement complexe dans ce contexte. Le fait qu'ils appartiennent à l'État et contrôlent généralement une grande partie de l'infrastructure de l'Internet les conduit à être moins indépendants de l'État que ce ne serait autrement le cas. Cela peut souvent avoir un effet défavorable sur le respect de la vie privée des internautes, particulièrement

---

59 Mueller (2010) Networks and States, Mueller, M. L. (2010). Networks and States: The Global Politics of Internet Governance, p. 150-151. MIT Press.

dans les pays où l'État ne se soucie guère de respecter la vie privée et plus généralement les droits de l'homme des internautes. Inversement, la privatisation des FAI appartenant à l'État ainsi que le dégroupage de la boucle locale (LLU) ont des chances de produire une structure du marché des FAI plus propice à la protection de la confidentialité.

Plus généralement, les FAI sont dans une position particulièrement difficile pour résister aux immixtions dans la vie privée de leurs clients car ils sont généralement tenus par des accords de licence qui les obligent à fournir des données aux organismes publics. Cela peut être parfaitement légitime dans certaines situations mais les désavantages par rapport aux autres intermédiaires de l'Internet qui risquent moins d'être contraints de fournir les données de leurs usagers. L'évolution du modèle d'affaires des FAI vers la fourniture de services et de contenus supplémentaires groupés aux internautes signifie que les FAI particulièrement importants sont beaucoup plus vulnérables à la coercition de la réglementation qu'ils ne l'étaient précédemment.

Cette évolution est encore accentuée par le fait qu'une grande partie des contenus supplémentaires groupés que les FAI peuvent offrir sont assujettis aux conditions contractuelles des titulaires de droits d'auteur, qui obligent alors les FAI à s'immiscer dans la vie privée des internautes en échange de l'accès exclusif aux contenus supplémentaires sur l'Internet. Quelques FAI du secteur mobile se félicitent même de cette évolution car ils ont déjà mis en place une infrastructure qui limite la confidentialité et ont en conséquence un avantage, en tant que « premiers arrivés », sur les autres FAI lorsqu'ils fournissent les données de leurs usagers à leurs parties. Comme l'a fait remarquer un représentant de FAI lors d'un entretien, il faut une singulière détermination pour résister aux demandes répétées des autorités publiques qui réclament les données des usagers.

Plus généralement, les arrangements de gouvernance nationaux et transnationaux ont fait qu'il est extraordinairement difficile d'endiguer le commerce international, très intrusif pour ce qui est de la vie privée, des données personnelles des individus, ou de prévoir des réparations efficaces des violations transfrontalières de la vie privée. Les intermédiaires transnationaux jouent de multiples rôles différents dans ces initiatives et il se peut qu'ils n'adhèrent pas toujours à une approche du respect de la vie privée fondée sur les droits. Trouver des mécanismes efficaces de protection des données et de la vie privée représente un des plus grands défis posés à la sauvegarde des droits de l'homme dans une société mondiale de l'information.

IV) Vie privée des enfants et des jeunes

Les préoccupations concernant le respect de la vie privée requièrent différents types de considérations pour différentes personnes[60]. Dans une récente étude, l'Agence européenne de cybersécurité a estimé que la protection de la vie privée des jeunes est une des stratégies clés de lutte contre la manipulation psychologique et le harcèlement en ligne[61]. Elle identifie les plates-formes Internet mal conçues et les niveaux de complexité inutilement élevés ainsi que le manque de

60 Hilles, L., et Jugendschutz.Net. (2011). Verlockt - Verlinkt - verlernt? Werbung, Vernetzung und Datenabfragen auf Kinderseiten. Mayence, Allemagne.

61 Marinos, L., & Agence européenne de cybersécurité. (2011). Cyber-bullying and online grooming: helping to protect against the risks. Heraklion, Grèce.

sensibilisation comme des vulnérabilités clés pour la vie privée des jeunes en ligne. En conséquence, une des principales recommandations de l'Agence est que « la création et l'utilisation de profils des usagers ne devraient pas être possibles pour les mineurs en général »[62], et qu'il faudrait instituer des sanctions financières plus sévères pour les entreprises qui enfreignent ces lois. Aux États-Unis, le Children's Online Privacy Protection Act [loi sur la protection de la vie privée des enfants en ligne] est destiné à garantir que les sites Internet obtiennent le consentement des parents avant de collecter des données de personnes âgées de moins de 13 ans. En conséquence, de nombreux sites Internet, dont Facebook, choisissent d'exclure de leur site Web les moins de 13 ans. Par ailleurs, les recherches universitaires donnent à penser que de nombreux parents aident leurs enfants à contourner les restrictions d'âge pour accéder à Facebook[63]. Cela pose clairement des questions quant à la capacité de la législation en vigueur à protéger la vie privée des enfants et des jeunes sur l'Internet.

2.2 Défis spécifiques posés par différentes applications, plates-formes de communication et modèles d'affaires

2.2.1 Informatique en nuage

L'informatique en nuage est un développement relativement récent dans lequel des volumes croissants de données – y compris de données personnelles – sont stockés dans un « nuage » en ligne. Lors du stockage, les données personnelles sont transmises sur l'Internet, ce qui constitue déjà un risque pour le contrôle individuel sur ces données. Une fois les données stockées dans le nuage, ces risques subsistent, par exemple un « fournisseur de nuage peut, sans en avertir un usager, déplacer les informations de celui-ci d'une juridiction à une autre, d'un fournisseur à un autre ou d'une machine à une autre »[64].

De plus, les données personnelles des usagers dans le nuage peuvent subir des modifications dynamiques en termes de services car « il est courant qu'une entreprise de l'Internet qui établit des conditions de service ou une politique de confidentialité se réserve le droit de modifier ces conditions ou cette politique sans limitation »[65]. Cette importante mise en garde signifie que dans bien des cas même une politique de confidentialité ou des « conditions de service » qui paraissent très protectrices des données personnelles peuvent être modifiées d'un jour à l'autre. Les usagers n'ont que des moyens limités pour réagir à ces changements et dans certains cas il se peut qu'ils ne soient même pas au courant ou soient incapables de comprendre les implications de ces changements pour leurs propres données personnelles.

---

62 Ibid., p. 47.

63 Boyd, D., Hargittai, E., Schultz, J., et Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the "Childrens Online Privacy Protection Act'. First Monday, 16(11).

64 Gellman, R., et World Privacy Forum. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Extrait de http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

65 Ibid.

La protection des données personnelles doit faire face au modèle d'affaires même de l'informatique en nuage, qui fondamentalement attend des usagers (et très souvent de leurs clients aussi) qu'ils transfèrent leurs données personnelles sur l'Internet. Ce faisant, les usagers abandonnent habituellement toute « souveraineté » sur les données, ce qui veut dire qu'ils ne pourront plus déterminer sous quelle juridiction peuvent se trouver leurs données. En outre, le contrôle centralisé de ces données par le fournisseur de nuage fait qu'elles sont assujetties à des algorithmes informatiques, ce qui peut révéler des informations personnelles que les usagers ne voulaient pas divulguer ou qu'ils ne connaissaient même pas. Cela permet aussi au fournisseur de nuage de corréler leurs données personnelles et de croiser ces données dans les bases de données de tiers. Les données stockées dans le nuage peuvent aussi faire l'objet d'une injonction d'un tribunal dans toute juridiction où le fournisseur du nuage emploie du personnel ou possède des actifs. Dans le cas particulier des grandes entreprises transnationales jouant le rôle de fournisseurs de nuages, on peut s'attendre que le nombre de gouvernements en mesure de demander d'accéder aux données stockées dans le nuage soit très élevé.

Il serait possible de remédier à beaucoup de ces problèmes en offrant des solutions robustes de cryptage aux usagers des services que fournit le nuage, à la fois lors de la transmission et une fois les données stockées. Ces mesures garantiraient que seul l'usager a accès à ses données personnelles. Cependant, aujourd'hui très rares sont les fournisseurs de nuage qui offrent ce niveau élevé de cryptage des données – à la fois lors de la transmission et une fois les données stockées. D'autre part, un débat est en cours dans la communauté de l'Internet sur la question de savoir si les fournisseurs de nuages sont dignes de confiance. Comme certains des plus grands fournisseurs de services de courriel continuent à stocker des informations personnelles dans le nuage sans crypter les données personnelles, les soupçons de la communauté de l'Internet ne paraissent pas dénués de fondement. Ces soupçons semblent confirmés alors que de grands services de l'Internet dans le nuage sont piratés et que la quantité de données personnelles apparaît clairement (voir l'encadré ci-après pour plus de détails).

V) 85 % des données personnelles des internautes perdues en République de Corée

À la mi-2011, les citoyens de la République de Corée ont enregistré la plus grande perte – et de loin – de données personnelles dans l'histoire du pays. SK Communications Co a informé le public que les informations personnelles de 35 millions de clients avaient été piratées, avec des données personnelles volées principalement sur son site de réseau social Cyworld et son moteur de recherche Nate, deux des plus importants sites Web de la République de Corée. Ces informations personnelles comprenaient des noms d'usagers, des mots de passe, des numéros de sécurité sociale, des numéros d'identification des résidents, des noms, des numéros de téléphone mobile, des adresses de courriel et des photographies personnelles[66]. Selon l'UIT, il y a environ 40 millions d'internautes en République de Corée, ce qui donne à penser que plus de 70 % des Coréens

66 Sung-jin, Y. (2011). 35m Cyworld, Nate users' information hacked. The Korea Herald. Extrait le 13 décembre 2011 de http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110728000881

ou près de 90 % de tous les internautes de la République de Corée se sont fait voler les informations personnelles stockées dans le nuage[67]. Avant l'attaque, le Gouvernement de la République de Corée avait une politique du « nom réel » qui obligeait les usagers des grands sites Web à utiliser leur nom réel et à fournir leur numéro de sécurité sociale pour prouver leur identité, mais le gouvernement a annoncé que cette politique serait modifiée à la suite de l'attaque et elle a finalement été infirmée par la Cour constitutionnelle coréenne en août 2012. Pourtant, le choc massif de l'atteinte aux données en République de Corée est une leçon pour l'industrie de l'Internet où le contrôle oligopolistique des données personnelles devient de plus en plus la norme.

Dans maintes situations, les fournisseurs de l'informatique en nuage sont vulnérables face aux décisions prises par les intermédiaires de l'Internet. Quel que soit le degré de protection promis par le fournisseur du nuage en termes de service, la sécurité et la confidentialité des informations personnelles dépendent en fin de compte du maillon le plus faible de la chaîne. Comme plusieurs intermédiaires sont généralement mêlés au transfert et au stockage des informations personnelles dans le nuage, il suffit qu'un seul commette une faute intentionnelle ou non pour que les informations personnelles soient divulguées[68]. D'autre part, les fournisseurs de nuage sont aussi vulnérables face aux programmes gouvernementaux de surveillance, car ils transfèrent de grandes quantités de données personnelles via l'Internet public afin de les stocker dans le nuage et ils peuvent dans bien des cas continuer à les transférer via l'Internet public entre différentes régions du nuage. Ces procédures font qu'il est pratiquement impossible à un utilisateur final de dire avec une certitude absolue à travers quelles juridictions ses données personnelles seront acheminées. En conséquence, il devient aussi très difficile aux utilisateurs de l'informatique en nuage de déterminer à quels programmes gouvernementaux de surveillance leurs données peuvent être assujetties.

Enfin, il y a beaucoup de problèmes juridiques non résolus concernant la protection des données personnelles dans le nuage. Comme « le nuage peut avoir simultanément plusieurs localisations juridiques, avec des conséquences juridiques différentes »[69], il est permis de se demander comment les fournisseurs de nuage réagiront dans tel ou tel contexte. L'informatique en nuage n'est pas intrinsèquement capable de protéger les données personnelles. Toutefois, un modèle d'affaires fondé sur la centralisation des données personnelles dans une plate-forme de traitement des données via un réseau de communications distribué va soulever des questions importantes sur la protection des données personnelles.

---

67 Telecommunications Research Centre. (2011). World telecommunication. Genève : UIT.

68 Filippi, P. de. (2011). Notes on Privacy in the Cloud.

69 Gellman, R., ey World Privacy Forum. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Extrait de http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

2.2.2 Moteurs de recherche

Les moteurs de recherche ont historiquement rempli une fonction importante sur l'Internet en aidant les internautes à naviguer dans les vastes ressources disponibles en ligne. Comme beaucoup de services Internet, ils sont gratuits, avec un modèle d'affaires fondé sur la publicité. Dans ces modèles d'affaires, les usagers ne paient pas d'argent mais paient en fournissant leurs données et en visionnant les publicités fondées sur ces données. Meilleures et plus complètes sont les données personnelles, et plus efficace peut être la publicité. En conséquence, il ne semble pas déraisonnable de considérer que les moteurs de recherche sur l'Internet sont conçus pour collecter autant de données personnelles que possible en raison de leur modèle d'affaires.

Les moteurs de recherche de l'Internet ont souvent élargi leurs services pour englober d'autres types de services tels que le courriel ou le partage d'images qui peuvent être proposés aux usagers. Ces services supplémentaires permettent aux moteurs de recherche de croiser les informations entre différents services et de construire ainsi des profils plus complets des usagers. Un effet d'intégration fait que les multiples services intégrés sont plus faciles à utiliser et plus intéressants pour les usagers, mais ceux-ci paient davantage de leurs données personnelles en offrant une vue à 360 degrés de leur vie personnelle. Un conflit similaire existe déjà en ce qui concerne la customisation, dans laquelle les usagers du moteur de recherche cèdent une partie de leur vie privée en échange d'une plus grande personnalisation des services de recherche. Dans ce cas la valeur du service peut augmenter, mais l'usager « paie » ce service amélioré en sacrifiant un petit peu plus de ses données personnelles.

Un autre fait nouveau notable a été la montée en puissance des « moteurs de recherche nationaux » en Chine, dans la Fédération de Russie et dans d'autres régions du monde. Ces moteurs de recherche ont défié les moteurs de recherche internationaux dominants avec un succès particulier dans certaines régions du monde, mais il y a dans la communauté de l'Internet une grande préoccupation concernant leurs pratiques en matière de confidentialité. Alors que les acteurs transnationaux peuvent être préparés à contester des pratiques plus restrictives pour les usagers en matière de confidentialité, les moteurs de recherche nationaux sont indissociablement liés à leurs marchés locaux clés. Cela les laisse à la merci des cadres réglementaires nationaux dans leurs marchés locaux respectifs. Dans la mesure où ceux-ci sont très soucieux de protection de la vie privée, cela pourrait être considéré comme un développement positif, mais ce n'est généralement pas le cas. D'autre part, il y a aussi des signes qui indiquent que la « concurrence fondée sur la confidentialité » pourrait se développer lentement entre moteurs de recherche. Un mélange de pressions des usagers, de la société civile et de la réglementation a fait que certains moteurs de recherche ont commencé à innover dans le domaine des politiques de confidentialité[70]. C'est un signe encourageant, car on peut espérer que la concurrence entre moteurs de recherche impulse une amélioration globale des politiques de confidentialité. Pourtant, il est permis de se demander si les pratiques connexes des moteurs de recherche sont vraiment en train de changer. Beaucoup d'informations sur les politiques de confidentialité fournies par les moteurs de recherche restent difficiles à évaluer et à vérifier.

---

70 Cooper, A. (2007). Competing on Privacy. Center for Democracy and Technology. Extrait le 13 décembre 2011 de https://www.cdt.org/blogs/alissa-cooper/competing-privacy.

Les moteurs de recherche restent des entreprises ayant affaire à des consommateurs, qui dépendent de la confiance des usagers et des consommateurs pour fonctionner. Une perte de confiance substantielle pourrait avoir des conséquences directes sur l'aptitude des moteurs de recherche à exister et à exercer une activité commerciale profitable. Dans la mesure où on peut espérer que le marché des recherches deviendra de plus en plus mature, la concurrence s'intensifiera entre les moteurs de recherche pour les inciter à démontrer activement leur engagement en faveur du respect de la vie privée des usagers. Cela ne veut pas dire qu'il n'y a pas d'effets de verrouillage, et il se peut que les usagers deviennent de plus en plus dépendants des moteurs de recherche. Certaines fonctions des moteurs de recherche telles que la vitesse, le lien aux réseaux sociaux ou aux comptes de courriel ont des chances d'être considérées comme faisant partie de l'expérience de la recherche par les consommateurs et seront de plus en plus attendues des autres fournisseurs de moteurs de recherche, relevant la barre pour ceux qui voudraient se faire une place sur ce marché. D'autre part, les effets de verrouillage paraissent très dépendants des pratiques de recherche habituelles, qui pourraient être changées assez rapidement si une violation grave de la confiance venait à se produire[71]. La confiance accordée aux moteurs de recherche remplace à bien des égards une compréhension plus sûre de la question de savoir si les contenus de l'Internet sont pertinents et dignes de foi[72]. À mesure que la maîtrise des médias se développe lentement dans le grand public, on pourrait espérer que la dépendance vis-à-vis des moteurs de recherche diminuera l'effet actuel de verrouillage, intensifiant ainsi la compétition sur d'autres questions clés comme la confidentialité.

2.2.3 Réseaux sociaux

Les effets de verrouillage notés dans certains moteurs de recherche et services connexes sont importants, mais ces effets peuvent être encore plus grands sur les réseaux sociaux (voir l'encadré ci-dessous pour plus de détails). S'il est vrai que « Facebook pourrait bien avoir réussi à devenir irremplaçable pour beaucoup de ses usagers »[73], cela a des implications substantielles pour la confidentialité sur l'Internet. En effet, les usagers sont vulnérables aux modifications unilatérales apportées par Facebook et aussi par d'autres réseaux sociaux à leurs politiques et pratiques en matière de confidentialité. Les usagers sont si captifs des réseaux sociaux que même s'ils désapprouvent dans le fond leurs politiques de confidentialité, ils ne risquent pas de quitter le réseau. Cela augmente substantiellement le pouvoir des réseaux sociaux sur la vie privée de leurs usagers.

Comme pour les moteurs de recherche, le modèle d'affaires des réseaux sociaux est fondé sur la publicité et il n'y a pas de relation financière directe entre les usagers des réseaux sociaux et ces réseaux eux-mêmes. Toutefois, les réseaux sociaux poussent

---

71 Voir Banwell, L., Ray, K., Coulson, G., Urquhart, C., Lonsdale, R., Armstrong, C., Thomas, R., et al. (2004). The JISC User Behaviour Monitoring and Evaluation Framework. Journal of Documentation, 60(3), 302-320 et Griffiths, J. (s.d.). Student searching behaviour and the Web: use of academic resources and google. Library trends, 2005, vol. 53, no. 4, p. 539-554, The Johns Hopkins University Press.

72 Voir Shaker, L. (2006, April 3). In Google we trust: Information integrity in the digital age. First Monday. Ghosh, Rishab Aiyer. Extrait de http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/1320/1240 et Hargittai, E. (2010). Trust online: young adults' evaluation of Web content. International Journal of Communication, 4.

73 York, J. C. (2010). Policing Content in the Quasi-Public Sphere. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University.

cette logique plus loin que les moteurs de recherche étant donné que les contenus qu'ils produisent sont aussi des contributions des usagers. Comme presque tous les contenus fournis par les usagers des réseaux sociaux sont des informations personnelles et des données privées, il ne paraît pas déraisonnable de penser que les usagers des réseaux sociaux échangent leurs données privées contre un service « monétairement gratuit ». Il existe pourtant des relations financières contractuelles entre les réseaux sociaux et leurs partenaires de la publicité, qui sont responsables du financement du réseau. En conséquence, les réseaux sociaux sont du point de vue commercial naturellement incités à constamment améliorer le ciblage de leur publicité à l'aide des données personnelles de leurs usagers. Il peut y avoir d'autres moyens de générer des recettes au sein des réseaux sociaux par des modèles d'abonnement ou de transactions, mais le gros des recettes de la plupart des grands réseaux sociaux continue à provenir de la publicité[74]. En conséquence, les données personnelles des usagers des réseaux sociaux sont toujours la monnaie clé, une masse critique qu'il faut obtenir pour que les réseaux sociaux demeurent profitables[75].

VI) Le pouvoir du verrouillage

« Le fait de disposer d'un lieu unique pour toute notre communication nous laisse à la merci des politiques de ceux qui contrôlent l'infrastructure à laquelle nous sommes enchaînés – Vous ne pouvez pas quitter Facebook sans quitter toutes vos connaissances – parce que tous les gens que vous connaissez sont sur Facebook. Je n'étais pas un usager de Facebook, j'étais hostile à Facebook. Je pensais qu'il était mauvais de centraliser toute notre communication en un seul lieu. Je n'aimais pas les implications pour la confidentialité. Je n'aimais pas la censure exercée par Facebook sur des choses comme les images de mères allaitantes […] je pensais que ces politiques étaient mauvaises et ma réaction consistait à ne pas rejoindre Facebook pendant des années alors que tous mes amis étaient sur Facebook […] J'ai rejoint Facebook à la fin de l'an dernier […] parce qu'un ami est mort. Il s'appelait Chuck ; c'était un homme brillant qui passait beaucoup de temps en ligne. Il était sur Facebook et partageait des choses avec ses amis sur Facebook – et quand il est mort je me suis aperçu que je n'avais pas communiqué avec lui depuis un certain temps […] je ne le rencontrais pas là où il était, je n'étais pas sur Facebook. J'ai manqué quelque chose d'énorme. Tel est le coût de ne pas y être – et j'ai donc rejoint Facebook parce que j'ai estimé qu'aussi fortes que soient mes convictions, il était plus important pour moi d'être là avec mes amis et de parler à mes amis. C'est le pouvoir du verrouillage »[76].

---

74 Pour une étude approfondie des modèles de financement des réseaux sociaux, voir Enders, A., Hungenberg, H., Denker, H.-P., et Mauch, S. (2008). The long tail of social networking. Revenue models of social networking sites. European Management Journal, 26(3).

75 Mueller, P. (2011). Offene Staatskunst - Strategie für eine vernetzte Welt. Arbeitskreis Internet Governance. Munich, Allemagne : Münchner Centrum für Governance-Forschung (MCG).

76 Vasile, J. (2011). Presentation of the FreedomBox. Elevate 2011 - Music, Arts and Political Discourse. Graz, Autriche : Verein zur Förderung des gesellschaftspolitischen und kulturellen Austausches.

On fait souvent valoir que les usagers des réseaux sociaux consentent explicitement à ces utilisations des données personnelles dans les conditions de service et la politique de confidentialité. Il se peut que cet argument dégage la responsabilité juridique des réseaux sociaux, mais un consentement éclairé ou de fond présupposerait que les usagers soient (1) conscients de la politique de confidentialité, (2) capables de comprendre le langage juridique complexe employé dans ces politiques, (3) disposés à prendre le temps de lire des politiques et (4) capables d'accepter certaines parties de la politique de confidentialité tout en en rejetant d'autres. Cependant, même si les usagers agissent ainsi, les politiques de confidentialité peuvent être modifiées à tout moment, ce qui fait que même l'usager le mieux informé est vulnérable aux modifications soudaines, inattendues et unilatérales apportées à la politique de confidentialité par les fournisseurs de réseaux sociaux[77]. Il a été estimé que cette instabilité du traitement des données privées est comparable à une situation dans laquelle « les locataires n'auraient aucun droit au respect de la vie privée chez eux parce qu'il se trouve qu'ils louent des murs et des portes. Cette semaine, vous avez la permission de fermer la porte, mais malheureusement pour vous nous avons modifié les conditions de service »[78].

Il y a aussi les questions associées à la mise en public pratiquée sur les réseaux sociaux qui va bien au-delà des réseaux sociaux eux-mêmes. C'est devenu une pratique courante des programmes automatisés d'exploiter les données personnelles livrées au public sur les sites des réseaux sociaux. En conséquence, il peut suffire que des données personnelles soient publiquement disponibles pendant un bref laps de temps pour qu'elles soient diffusées sur beaucoup d'autres sites, espaces en ligne et systèmes techniques[79]. Ce risque peut exister de façon similaire pour d'autres services Internet, mais la simple quantité de données personnelles stockées sur les sites des réseaux sociaux fait que le risque d'une mise en public inopinée de données privées est bien plus grand que pour d'autres services comparables. Ces problèmes sont aggravés par les opérations quotidiennes de nombreux sites de réseaux sociaux qui sont généralement conduites par des informaticiens et des ingénieurs. Dans ce contexte, les produits et services sont mis au point selon une logique d'ingénierie consistant à fournir aux clients les nouveaux produits les plus perfectionnés et une politique de confidentialité est ensuite plaquée au dernier moment. Dans toutes les recherches effectuées pour le présent rapport, cette dimension d'organisation interne au sein des réseaux sociaux n'a cessé de réapparaître comme un obstacle majeur à la mise en place de protections plus efficaces de la vie privée des usagers.

---

77 Electronic Privacy Information Center. (2011). Social Networking Privacy. Extrait le 13 décembre 2011 de https://epic.org/privacy/socialnet/.

78 Tufekci, Z. (2010). Facebook: The Privatization of our Privates and Life in the Company Town. Technosociology: Our Tools, Ourselves. Extrait le 13 décembre 2011 de http://technosociology.org/?p=131.

79 Pour une vue d'ensemble des problèmes et des solutions, voir Fuchs, C. (2009). Social networking sites and the surveillance society a critical case study of the usage of studiVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance. Salzbourg: Forschungsgruppe Unified Theory of Information.

2.2.4 Téléphones mobiles, smartphones et Internet mobile

L'explosion de l'utilisation de l'Internet mobile au XXIe siècle a contribué à beaucoup des préoccupations actuelles concernant la confidentialité et la protection des données sur les réseaux de téléphonie mobile. En comparaison avec les communications sur ligne fixe, les communications mobiles présentent plusieurs attributs qui ont un effet particulièrement négatif sur la confidentialité. Ces attributs comprennent le numéro international unique d'identification d'appareil mobile (IMEI) et le numéro unique de carte SIM (IMSI), l'aptitude à déterminer régulièrement la localisation géographique des appareils mobiles et l'aptitude des tiers à intercepter les communications mobiles sans fil lors de leur transmission[80]. Ces préoccupations pour la confidentialité qui concernent spécifiquement l'Internet mobile doivent toutes être prises en considération en sus des préoccupations existantes pour la confidentialité sur l'Internet qui s'appliquent aussi aux appareils mobiles connectés à l'Internet.

S'il est fréquemment présumé que ces préoccupations ne s'appliquent qu'aux « smartphones », elles s'appliquent tout autant à tout appareil mobile capable d'accéder à l'Internet via les réseaux de téléphonie mobile. En conséquence, il faut prendre en considération ces préoccupations tenant à la confidentialité dans le monde en développement et le monde développé pour tout appareil capable d'accéder à l'Internet. Elles s'appliquent aussi bien à un agriculteur du Zimbabwe qui envoie des courriels à sa famille sur un vieux téléphone Nokia qu'à un avocat d'affaires à Hong Kong qui se sert d'un iPhone pour envoyer un courriel à un client. Ces préoccupations existent déjà en ce qui concerne la téléphonie mobile en général, mais elles sont encore aggravées par l'utilisation de l'Internet sur les appareils mobiles.

Cependant, au-delà des préoccupations spécifiques pour la confidentialité concernant les réseaux mobiles eux-mêmes, les smartphones posent plus de problèmes de confidentialité que les téléphones mobiles moins intelligents. Les smartphones sont généralement utilisés comme appareils de l'Internet mobile et sont habituellement capables de transférer des quantités beaucoup plus grandes de données que les téléphones mobiles ordinaires grâce à ce qu'on appelle les réseaux de téléphonie mobile de deuxième (2G), troisième (3G) et quatrième (4G) génération. Cela veut dire qu'ils sont aussi capables de transférer beaucoup plus de données personnelles sur l'Internet public qu'un téléphone mobile ordinaire. De plus, ces téléphones sont conçus pour être constamment connectés à l'Internet. Enfin, divers services sont intégrés dans les smartphones, qui envoient régulièrement des informations sur l'Internet, souvent à l'insu de l'utilisateur du téléphone. Il a été établi que tant les smartphones Android de Google que l'iPhone d'Apple « téléphonent chez soi » régulièrement, transférant ainsi des informations sur leur localisation, sur leur utilisateur et autres informations potentiellement personnelles comme les réseaux WiFi accessibles sur l'Internet[81].

---

80 Electronic Frontier Foundation (EFF). (2011). Mobile Devices. Surveillance Self-Defense Project. Retrieved December 13, 2011, from https://ssd.eff.org/tech/mobile.

81 Angwin, J., ey Valentino-Devries, J. (2011). Apple's iPhones and Google's Androids Send Cellphone Location. Wall Street Journal. Extrait le 13 décembre 2011 de http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

Cela contribue encore à la tendance globale de la confidentialité des smartphones, à savoir la fragmentation du contrôle des données personnelles dans les plates-formes de l'Internet mobile. Le prestataire de services d'Internet mobile, le fournisseur du système d'exploitation et les fournisseurs d'applications ont tous un certain niveau de contrôle sur les données personnelles des usagers. Dans le cas d'un utilisateur type du smartphone qui envoie des courriels en Argentine, certaines de ses données personnelles pourraient être contrôlées par le fabricant de l'appareil (Samsung), le fournisseur du système d'exploitation du mobile (Google), le prestataire des services de l'Internet mobile (Movistar), le fournisseur de l'application courriel (K-9 Mail), le prestataire de services de courriel (Yahoo) et le prestataire de services de courriel du destinataire des courriels (Microsoft). Cela n'inclut même pas les problèmes de fuite de données lorsque des mots de passe et des contenus de courriels sont envoyés sans cryptage sur l'Internet, l'accès supplémentaire potentiel aux données personnelles par les autorités locales ou internationales ou l'accès à ces données de tiers non autorisés. N'est pas non plus pris en considération le niveau supplémentaire de complexité introduit par l'installation d'applications additionnelles des smartphones (« Apps »), qui peuvent aussi avoir accès aux données personnelles des usagers. De plus, les smartphones combinent un vaste ensemble de capteurs, de puces et de plates-formes de communication, ce qui fait qu'il est difficile aux utilisateurs des smartphones de comprendre les implications pour la confidentialité de chaque capteur additionnel ou puce spécifique de communication. L'iPhone le plus récent, le 4S, comprend des puces de communication capables de communiquer sur différents types de réseaux de téléphonie mobile (GSM/CDMA/EDGE/UMTS/HSDPA/HSUPA), les réseaux « WiFi » de l'Internet (802.11b/g/n), les systèmes de positionnement global GPS et la technologie Bluetooth, ainsi qu'un capteur de lumière, un capteur de proximité, un capteur de mouvement (gyroscope) et de multiples microphones[82].

VII) Exploitation des informations stockées dans les appareils connectés à l'Internet

Dans beaucoup d'États répressifs à travers le monde, c'est une pratique habituelle de forcer les prisonniers politiques qui ont été arrêtés à remettre leurs appareils connectés à l'Internet avant d'être interrogés. Les autorités s'intéressent particulièrement aux smartphones, vu que ceux-ci transportent quantité de données privées qui ne sont normalement pas disponibles sur les téléphones mobiles ordinaires. Ces informations personnelles sont ensuite utilisées pour recueillir systématiquement des informations sur les réseaux sociaux que fréquentent les prisonniers politiques. Avec ces informations, il est possible de cibler d'autres contacts directs et indirects des prisonniers politiques. Ces réseaux comprennent les réseaux personnels, professionnels et occasionnels d'individus qui sont eux-mêmes intimidés ou emprisonnés le plus souvent pour la simple raison qu'ils ont rencontré – même brièvement – la personne qu'il ne fallait pas. Ces méthodes ne répondent pas nécessairement à un objectif légitime du gouvernement ; elles servent plutôt à intimider les individus et leurs réseaux personnels. Elles

82 Higginbotham, S. (2010). iPhone 4 Sensors Highlight a Bright Spot for VCs. GigaOM. Extrait de http://gigaom.com/2010/06/08/iphone-4-sensors-highlight-a-bright-spot-for-vcs/.

peuvent être manipulées pour produire des effets paralysants et étendre l'ombre de la hiérarchie de l'État bien au-delà des prisonniers politiques eux-mêmes. Les appareils de communication personnelle et les données personnelles ainsi numérisées et collectées sont indispensables à ces stratégies d'intimidation.

Ces capteurs peuvent être combinés selon des modalités inattendues, comme les récentes tentatives pour enregistrer ce que l'usager dactylographie à l'aide du capteur à mouvement de gyroscope[83]. Une grande partie des données collectées sur les smartphones est stockée sur le téléphone pendant une durée non spécifiée, et l'usager n'a guère de contrôle sur leur existence ou leur suppression. Selon le contexte dans lequel ils sont utilisés, les smartphones peuvent devenir rapidement des dépositaires numériques de la vie de leur propriétaire. Cela veut dire que si les smartphones sont perdus, volés ou simplement pris à leur propriétaire, les implications pour la vie privée des individus peuvent être graves (voir l'encadré pour en savoir plus).

Enfin, les deux plates-formes de smartphones dominantes, l'Android de Google et l'iPhone d'Apple, utilisent aussi leurs plates-formes respectives de téléphonie mobile pour cibler la publicité sur les usagers. Dans bien des cas, les données que ces sociétés ont obtenues d'autres appareils connectés à l'Internet sur leurs utilisateurs – au moyen de l'historique de leurs recherches sur Google, de l'historique de leurs achats sur iTunes Store, de l'historique de leur utilisation de leur compte Apple/Google – peuvent être combinées avec les données fournies par la plate-forme mobile telles que les données de localisation géographique provenant du téléphone. Ces informations personnelles sur un individu – qui peuvent dans bien des cas être plus étendues que ce que savent les usagers eux-mêmes – permettent à ces plates-formes de cibler sur leurs usagers des publicités très personnalisées. Comme dans le cas des moteurs de recherche et des réseaux sociaux, les concepteurs des plates-formes de l'Internet mobile ont un intérêt commercial à obtenir le maximum d'informations personnelles de leurs usagers. Plus elles en savent sur leurs usagers, plus rentable a des chances d'être la publicité ciblée sur les plates-formes de l'Internet mobile.

2.2.5 Identificateurs uniques des citoyens et initiatives de gouvernance en ligne

Bien avant l'apparition de l'Internet public au début des années 1990, les gouvernements à travers le monde ont pris des mesures pour normaliser et centraliser les pièces d'état-civil de leurs citoyens. À mesure que la puissance de calcul a augmenté et que les coûts ont diminué, les États ont pu améliorer l'efficience de leurs administrations en centralisant et en normalisant les informations sur leurs citoyens[84]. Conformément aux vues de James C. Scott, les États ont cherché à rendre « lisibles » les sociétés qu'ils gouvernent afin de promouvoir leurs politiques[85]. Ces gains d'efficience servent aussi à répondre aux

83 Cai, L., et Chen, H. (2011). TouchLogger: inferring keystrokes on touch screen from smartphone motion. HotSec'11 Proceedings of the 6th USENIX conference on Hot topics in security. Berkeley, CA, USA: USENIX Association.

84 Pour une étude sur l'importance de l'informatique pour les États et les sociétés modernes, voir Robertson, D.S. (1998) The New Renaissance: Computers and the Next Level of Civilization. Oxford University Press, États-Unis.

85 Scott, J.C. (1998) Seeing like a state : how certain schemes to improve the human condition have failed. New Haven: Yale University Press.

demandes insistantes tendant à ce que les administrations publiques réduisent les coûts en augmentant l'efficience par l'informatisation. Ces gains d'efficience ont souvent un impact négatif sur la vie privée et l'anonymat des citoyens. Les initiatives publiques visant à créer de grandes bases de données publiques sur les citoyens ont été accueillies avec scepticisme par les défenseurs du respect de la vie privée. Les dangers de ces bases de données sont particulièrement évidents lorsque des informations sont perdues (voir l'encadré pour plus de détails).

Ces bases de données et services d'identification incluent souvent une composante en ligne, permettant aux citoyens d'accéder à divers services publics via l'Internet. L'utilisation de ces services peut beaucoup apporter aux citoyens, par exemple une plus grande commodité et une plus grande efficience. Mais comme l'a noté un Groupe de travail sur la protection de la vie privée du Gouvernement des États-Unis :

« Ces avantages ne vont cependant pas sans une contrepartie : la moindre protection de la vie privée. Il s'agit dans ce contexte de la confidentialité de l'information, du droit de l'individu de contrôler les conditions dans lesquelles les informations personnelles – les informations rattachables à un individu – sont acquises, divulguées et utilisées »[86].

VIII) Perte des données personnelles de 25 millions de citoyens

Une des plus grandes pertes de données sur les citoyens survenues en Europe a touché le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, où deux CD contenant les données personnelles de plus de 25 millions d'individus ont été perdues dans le système postal interne du gouvernement en 2007[87]. Ils ont été envoyés sans aucun mécanisme de protection technique par le British Revenue and Customs Service (HRMC) au National Audit Office (NAO). De plus, le niveau du contrôle gouvernemental effectif sur le transport des CD est sujet à caution, étant donné que le transport a été effectué par un service privé. Les informations personnelles figurant sur les CD concernaient les paiements d'allocations familiales à toutes les familles du Royaume-Uni. Comme la très grande majorité des familles au Royaume-Uni ont droit à des allocations familiales, la perte de données personnelles a touché presque toutes les familles comprenant des enfants de moins de 16 ans. Il a été indiqué au Royaume-Uni que la majorité des pertes importantes de données personnelles sont survenues dans le secteur public[88]. Cela est généralement imputé à l'échec de la tentative de « promouvoir une culture de la sécurité des données personnelles »[89], tant en ligne que hors ligne.

86 Gates, J., et Privacy Working Group. (1995). Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information. Information Policy Committee, Information Infrastructure Task Force. Extrait de http://aspe.hhs.gov/datacncl/niiprivp.htm.

87 Gorge, M. (2008). Data protection: why are organisations still missing the point? Computer Fraud & Security, 2008(6), 5-8.

88 Privacy International. (2011). United Kingdom - Privacy Profile. Privacy International. Extrait le 13 décembre 2011 de https://www.privacyinternational.org/article/united-kingdom-privacy-profile.

89 Ibid.

Cette déclaration lucide décrit précisément la difficulté de faire en sorte que la gouvernance en ligne soit efficace tout en garantissant la protection de la vie privée. Cette tension peut aussi être trouvée dans les formes les plus récentes de gouvernance en ligne. Généralement, ces initiatives visent à accroître la participation des citoyens et la transparence des activités gouvernementales, mais là aussi il peut y avoir des préoccupations quant au respect de la vie privée. D'abord, il est généralement demandé aux usagers participant à ces initiatives de s'identifier en tant que citoyens dans les initiatives de gouvernance participative, étant donné que les non-citoyens ne peuvent normalement pas participer. De plus, il est attendu d'eux qu'ils participent à ces initiatives avec leur « identité intégrale ». La participation anonyme ou sous pseudonyme – même pour les individus identifiés comme citoyens – n'est généralement pas une option.

Un autre point important est la tension entre la transparence et les initiatives de gouvernance ouverte ou participative, et la confidentialité. La plupart des initiatives de gouvernance participative exigent un niveau élevé de transparence afin de garantir la légitimité du processus. Toutefois, ce faisant, elles risquent de restreindre excessivement les droits des individus à leurs données personnelles afin de sauvegarder la transparence. Exiger des citoyens qu'ils signent des pétitions ou participent à la gouvernance ouverte en utilisant leur nom réel résout les problèmes d'authentification pour le gouvernement qui utilise le système, mais conduit les utilisateurs à parler moins ouvertement que s'ils parlaient sous le couvert de l'anonymat ou d'un pseudonyme par l'intermédiaire d'un tiers digne de confiance.

Enfin, il est important de prendre en considération l'étroite coopération avec le secteur privé dans de nombreuses initiatives de gouvernance en ligne ou de gouvernance ouverte. Comme souvent les gouvernements n'ont pas les moyens de remplir eux-mêmes ces fonctions, ils externalisent fréquemment des processus et des services faisant partie intégrante des gouvernements modernes en s'adressant à des fournisseurs de services privés. Cela peut être un moyen efficace de réduire les coûts, mais crée aussi des risques accrus pour la confidentialité en associant des tiers au traitement, au transfert et au stockage des données personnelles des citoyens. Ces interactions avec le secteur privé ne nuisent pas nécessairement à la protection de la vie privée des citoyens, mais elles introduisent un niveau supplémentaire de complexité qui a besoin d'être gouverné de façon appropriée.

2.3 Menaces résultant de différents mécanismes de surveillance et de collecte des données

2.3.1 Identification des usagers – identificateurs uniques, cookies et autres formes d'identification des usagers

Il y a de multiples moyens d'identifier les internautes. De l'enregistrement initial des internautes par les fournisseurs d'accès à l'Internet aux cybercafés, à la numérotation et à l'identification des appareils Internet qui sont eux-mêmes souvent reliés à des comptes Internet, aux identificateurs individuels fournis par les navigateurs ou stockés sous la forme de cookies, ainsi qu'aux adresses IP qui sont assignées aux internautes par les protocoles de l'Internet. Toutes ces procédures d'identification peuvent servir à rendre un internaute moins anonyme, mais parfois ces identités peuvent aussi être nécessaires pour

fournir des services sur l'Internet. Il est difficile d'utiliser l'Internet sans adresse IP – même si, bien entendu, une adresse IP peut être assignée dynamiquement ou anonymisée – et de nombreux autres services Internet reposent sur une forme d'identification.

Surtout dans le monde en développement, mais aussi dans certaines régions du monde développé, l'enregistrement des internautes, à la fois pour l'utilisation de l'Internet à court terme et à long terme suscite une préoccupation importante en ce qui concerne la confidentialité. L'identification des usagers peut intervenir dans le cadre des procédures d'enregistrement d'un cybercafé, dans le cadre de la procédure de souscription à un réseau sans fil ou durant l'achat d'un contrat de téléphonie mobile. Dans chacun de ces contextes, les mécanismes d'identification des internautes contribuent à restreindre la confidentialité et l'anonymat sur l'Internet. Une autre cause de préoccupation est la restriction qui en résulte en ce qui concerne l'anonymat du discours et les effets d'intimidation dont s'accompagnent ces mécanismes d'identification. Certes ces procédures d'identification sont au moins relativement transparentes pour les internautes, ce qu'on ne peut dire des autres mécanismes d'identification des usagers.

Parmi les mécanismes d'identification des internautes les moins transparents, les cookies sont peut-être les plus connus. Ils sont stockés sur l'ordinateur d'un internaute quand il visite un site Web, et le navigateur de l'usager. Selon le mode de construction du site Web et les paramètres des navigateurs des internautes, de un à une douzaine de cookies peuvent être stockés lors de la visite d'un site Web. En stockant des cookies sur les ordinateurs des usagers, il est possible de suivre un internaute sur l'Internet. Surtout dans le cas des cookies qui sont extérieurs au domaine que visite l'internaute – les cookies dits de tiers – ces cookies peuvent « suivre » les internautes à travers la plupart des régions de l'Internet.

Les cookies sont aussi un élément de l'analyse des usagers, pratique couramment utilisée pour suivre les usagers sur l'Internet. Selon des estimations crédibles, de 40 à 60 % des plus grands sites de l'Internet utilisent Google Analytics, outil de suivi du trafic qui permet aux administrateurs du Web d'évaluer leur trafic[90]. Sur tous les sites Web de l'Internet, des estimations similaires donnent à penser que près de 70 % utilisent une forme ou une autre de suivi des internautes fondée sur différents systèmes d'analyse de l'Internet[91].

La mise en œuvre technique des cookies a depuis longtemps dépassé le point où les usagers ont un quelconque contrôle réel sur ce que suivent les cookies. Ceux-ci sont souvent installés durant des années sur l'ordinateur d'un internaute et sont reconduits automatiquement chaque fois que l'usager visite un site Web connexe. Ils peuvent aussi être installés par des modules de navigateurs tels que « Adobe Flash » indépendamment du navigateur principal. Si un internaute essaie de supprimer les cookies d'un des nombreux emplacements où ils peuvent être stockés, ils sont recréés à partir d'autres zones de stockage ou en utilisant d'autres mécanismes d'identification tels que les identificateurs de session, les modules de navigateur, les scripts de cache des cookies ou autres méthodes permettant de recréer les cookies sans le consentement des usagers

---

90 BuiltWith. (2011). Google Analytics Usage Statistics - Websites using Google Analytics. Extrait le 13 décembre 2011de http://trends.builtwith.com/analytics/Google-Analytics.

91 W3Techs. (2011). Usage Statistics and Market Share of Traffic Analysis Tools for Websites. Q-Success Web-based Services. Extrait le13 décembre 2011de http://w3techs.com/technologies/overview/traffic_analysis/all.

individuels[92]. Bien qu'il y ait eu de longs débats sur les soucis de confidentialité associés aux cookies relativement tôt dans l'évolution de l'Internet public, nombre des questions soulevées à ce propos ne sont toujours pas résolues[93].

Les cookies ne sont néanmoins qu'un des multiples éléments de l'identification des usagers sur l'Internet. Ils ont pour moteur le modèle fondé sur la publicité qui imprègne une grande partie de l'Internet et prospère sur l'identification des usagers aux fins du ciblage de la publicité. Si la customisation des sites Web et une plus grande pertinence des publicités sont fréquemment mentionnées comme des incitations offertes aux usagers pour qu'ils acceptent ou même appuient le suivi sur l'Internet, le fait que les usagers sont suivis sur l'Internet est conforme à une claire logique de profit. Les réactions outragées de l'industrie de la publicité sur l'Internet aux récentes lois de lutte contre le suivi adoptées dans différentes régions du monde ne sont qu'un exemple de ces intérêts commerciaux[94]. Alors qu'une bonne partie de l'industrie de l'Internet dépend des recettes publicitaires pour son financement, trouver des moyens d'éviter l'identification des usagers et le suivi en ligne, qui nuisent à la confidentialité, restera une tâche très délicate[95].

2.3.2 Publiciels, espiogiciels et logiciels malveillants conduisent une exploitation et une surveillance clandestines des données

D'autres menaces pèsent sur la confidentialité des opérations des usagers sur l'Internet du fait des publiciels, des logiciels malveillants et des virus. Dans certains cas ces programmes collectent des informations personnelles des internautes par exemple en volant de l'argent aux individus, en s'emparant de leurs comptes Internet ou en utilisant d'une autre manière abusive leurs informations personnelles. Une autre utilisation courante des espiogiciels est celle de l'usager qui désire observer clandestinement d'autres usagers qu'il connaît personnellement. Ces « espiogiciels » sont souvent utilisés par des harceleurs qui veulent s'immiscer dans la vie personnelle de leurs victimes. Cela peut inclure l'obtention de détails sur l'endroit où se trouve une personne, ses communications, d'autres informations personnelles et ses mots de passe[96]. Ce qui peut sembler surprenant, c'est qu'il est entièrement légal d'acheter et de vendre ces technologies dans beaucoup de régions du monde. Il est donc relativement facile à des individus qui veulent faire un usage abusif de ces technologies d'y avoir accès.

Les publiciels appartiennent aussi à la catégorie des logiciels qui envahissent la vie privée et font fi du consentement, logiciels qui sont stockés sur les ordinateurs à l'insu de leur propriétaire. Il est souvent très difficile aux internautes de reconnaître ces logiciels étant donné qu'ils se dissimulent sous l'apparence d'un programme anti-virus, d'un outil de

---

92 Mayer, J. (2011). Tracking the Trackers: Microsoft Advertising. Center for Internet and Society (CIS), Stanford Law School. Extrait le 13 décembre 2011 de http://cyberlaw.stanford.edu/node/6715.

93 On peut trouver une analyse plus approfondie dans RFC 2109: https://www.ietf.org/rfc/rfc2109.txt.

94 Clarke, G. (2011). Do-Not-Track laws gain US momentum. The Register. Extrait le 13 décembre 2011 de http://www.theregister.co.uk/2011/05/06/senate_do_not_track/.

95 Rooney, B. (2011). U.K. Publishes EU "Cookie" Directive Guidelines. Wall Street Journal. Extrait le13 décembre 2011 de http://blogs.wsj.com/tech-europe/2011/05/09/u-k-publishes-e-u-cookie-directive-guidelines/.

96 Electronic Privacy Information Center. (2011). Personal Surveillance Technologies. Extrait le 13 décembre 2011 de https://epic.org/privacy/dv/personal_surveillance.html.

recherche ou d'une technologie « utile » similaire. Ils accompagnent souvent un logiciel qui paraît libre. Toutefois, ce logiciel est en fait utilisé pour montrer des publicités à l'internaute et suivre ses comportements sur l'ordinateur.

De plus en plus pertinente, dans ce contexte, est l'utilisation par les autorités de police de la technologie du cheval de Troie pour recueillir des informations d'ordinateurs distants. Ces utilisations sont très controversées dans de nombreuses régions du monde étant donné qu'elles impliquent souvent la prise de contrôle de tout l'ordinateur. Cette technologie est alors utilisée comme une forme d'« interception juridique » ; cependant, la société civile la considère comme relevant des logiciels malveillants, tandis que les vendeurs de logiciels antivirus la classent dans les virus[97]. Ces utilisations ne laissent guère de place aux données personnelles privées qui sont stockées sur les ordinateurs, même si cet espace de « profonde intimité personnelle » est explicitement protégé comme un élément important de la dignité humaine dans de nombreux pays à travers le monde. Enfin, les logiciels malveillants, espions et publicitaires sont de plus en plus ciblés sur les appareils mobiles convergents tels que les smartphones, les tablettes et autres appareils connectés à l'Internet tels que les télévisions connectées (smart TV). Les usagers de ces appareils s'attendent à être en sécurité et ne demandent pas de protection supplémentaire. Perdre ses données personnelles sur un appareil qui n'est pas, à l'évidence, un ordinateur personnel est souvent inattendu (voir l'encadré pour plus de détails).

Les divers protocoles de communications utilisés par ces appareils offrent aux logiciels malveillants de multiples mécanismes de distribution différents. Un virus téléchargé sur l'Internet via un signal de téléphone mobile 3G peut être redistribué via un réseau sans fil WiFi ou Bluetooth à d'autres appareils à proximité immédiate. Comme les systèmes communs de fonctionnement des appareils mobiles tels que iOS et Android prolifèrent, il devient plus facile à ces appareils de propager les logiciels malveillants à des appareils aux systèmes d'exploitation similaires. La multiplicité des méthodes de communication et le manque de clarté des procédures de sécurité font des nouveaux appareils Internet des proies évidentes pour les logiciels malveillants et les publiciels. Vu que le nombre d'appareils connectés à l'Internet augmente rapidement, des consoles de jeu aux téléviseurs, voitures, fours à micro-ondes, réfrigérateurs connectés, et que l'« Internet des objets »[98] devient la norme, il est de plus en plus difficile aux usagers de contrôler leurs données personnelles. Les voitures et les télévisions connectées à l'Internet ne sont généralement pas des environnements privés permettant aux internautes d'installer un programme antivirus ou un pare-feu. Ces développements posent de sérieux défis au respect de la vie privée des usagers et à l'aptitude des individus à exercer un contrôle sur leurs données personnelles.

---

97 Chaos Computer Club. (2011). Chaos Computer Club analyse les logiciels malveillants d'origine gouvernementale. Extrait le 13 décembre 2011 de http://ccc.de/en/updates/2011/staatstrojaner.

98 Gershenfeld, N., Krikorian, R., et Cohen, D. (2004). The Internet of Things. Scientific American, 291(4), 76-81. Springer.

IX) Un réseau de consoles de jeu piraté

En avril 2011, le « Playstation Network » de Sony, qui est relié à la console Playstation de Sony, a été victime d'une intrusion commise par des agresseurs non identifiés. En conséquence, il a été estimé que les données personnelles de 77 millions d'utilisateurs du Playstation Network ont été compromises, dont leur nom, adresse, pays, adresse électronique, date de naissance et numéro de carte de crédit, ainsi que l'identifiant, le mot de passe et les réponses aux questions de sécurité du mot de passe utilisés sur le réseau[99]. Sans parler du volume des informations personnelles volées, il a fallu plus d'une semaine à Sony pour informer les usagers du réseau que leurs données personnelles étaient en danger. Comme l'utilisation d'un même mot de passe sur de multiples sites Internet est courante, cela a laissé les utilisateurs du Playstation Network en danger non seulement sur le réseau lui-même, mais aussi sur tout l'Internet.

2.3.3 Inspection approfondie des paquets (DPI)

La technologie de l'inspection approfondie des paquets est généralisée et elle est utilisée comme technologie générique de contrôle de l'Internet dans beaucoup de composantes de l'Internet. La technologie elle-même a la capacité d'« inspecter » les paquets qui voyagent à travers l'Internet, d'examiner leur contenu et d'y réagir par différents moyens. Historiquement, les technologies qui scannent et parfois modifient le trafic sur l'Internet ne le faisaient que sur la base d'informations d'en-tête. En revanche, l'inspection approfondie des paquets regarde « à l'intérieur » du paquet et le scanne pour certains mots clés, configurations ou autres caractéristiques que ne fait pas apparaître un examen des informations d'en-tête du paquet[100]. Si la DPI combine « maintes caractéristiques de technologies de l'Internet qui existent depuis longtemps, […] la combinaison de ces éléments est généralement considérée par l'industrie, les spécialistes de la technologie et les critiques des politiques comme une nouvelle technologie »[101]. C'est aussi une technologie qui est controversée depuis les premiers débats publics auxquels elle a donné lieu. Dans ces débats, la technologie a été associée à certaines des intrusions majeures dans la vie privée sur l'Internet. Lorsqu'il a été demandé à un vendeur de DPI, lors d'un entretien conduit par l'auteur, à quoi ressemblait la vente de matériel de DPI, il a répondu que c'était comme avoir une maladie sexuellement transmissible.

---

99 Stuart, K. (2011). PlayStation Network hack: what every user needs to know. The Guardian. Extrait le 13 décembre 2011 de http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/psn-security-advice.

100 Pour un examen détaillé des types de technologie d'inspection approfondie des paquets, voir Mueller, M. (2011). DPI Technology from the standpoint of Internet governance studies: An introduction. Syracuse University. Extrait de http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf.

101 Mueller, M. (2011). DPI Technology from the standpoint of Internet governance studies: An introduction. Syracuse University. Extrait de http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf.

Deux des premières utilisations de la technologie de l'inspection approfondie des paquets qui ont attiré l'attention du public étaient des publicités ciblées de Phorm et NenuAd. La technologie était employée pour construire des profils publicitaires détaillés sur les usagers de plusieurs fournisseurs d'accès à l'Internet, ce qui dans certains cas allait jusqu'à l'insertion de publicités additionnelles dans les sites Web. Cette manipulation active des sites Web des usagers et la collecte de leurs données sans leur consentement ont causé un tel scandale que la technologie a finalement été abandonnée par les fournisseurs d'accès à l'Internet en question et a été soumise à la justice[102]. Cela n'a guère encouragé une perception favorable par le public de cette technologie, qui a depuis lors été étroitement associée à des violations de la vie privée dans les débats publics. Dans le contexte de vastes contestations publiques en République islamique d'Iran et dans la région MENA (Moyen-0rient et Afrique du Nord) en 2009, 2010 et 2011, il a aussi été largement rapporté que la technologie de l'inspection approfondie des paquets était utilisé par les gouvernements pour surveiller et censurer leurs citoyens[103].

Depuis ces premières indications, des éléments d'information bien documentés ont continué d'être publiés ; ils rattachent la technologie de l'inspection approfondie des paquets à certains régimes de surveillance dans la région MENA. En dehors de cette région, l'inspection approfondie des paquets fait couramment partie des systèmes publics de surveillance, qui sont parfois qualifiés d'« interception licite ». Ils rendent toutes les informations non cryptées qui passent par les réseaux de communications visibles aux opérateurs de l'équipement, leur permettant de stocker et même dans certains cas de modifier les informations dans le réseau[104].

Une autre utilisation courante de la technologie de l'inspection approfondie des paquets consiste à profiler les usagers des réseaux de communications. Bien qu'il soit difficile de déterminer l'étendue de ce profilage, il est clair qu'il a des fins commerciales. Cependant, dans certains cas, il se peut fort bien que ces profils soient utilisés à des fins publicitaires pour cibler des publicités particulièrement pertinentes sur les usagers du réseau. Une autre forme d'utilisation de la DPI potentiellement invasive de la vie privée est le filtrage des contenus sur l'Internet, généralement parce que ces contenus sont jugés illégaux. Dans bien des cas, cela permet aussi de surveiller les usagers qui voudraient accéder à des contenus filtrés.

---

102 Commission européenne (2010). Stratégie numérique : la Commission saisit la Cour de justice d'un recours contre le Royaume-Uni en ce qui concerne la protection de la vie privée et des données à caractère personnel [IP/10/1215]. Extrait le 13 décembre 2011 de http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215.

103 Voir Silver, V., et Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. Bloomberg. Extrait le 28 août 2011de http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html et Sonne, P., et Coker, M. (2011). Foreign Firms Helped Gadhafi Spy on Libyans. Wall Street Journal. Extrait le 23 septembre 2011 de http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html.

104 Commission européenne (2010). Stratégie numérique : la Commission saisit la Cour de justice d'un recours contre le Royaume-Uni en ce qui concerne la protection de la vie privée et des données à caractère personnel [IP/10/1215]. Extrait le 13 décembre 2011 de http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215.

La DPI peut notamment être utilisée pour la gestion de la bande passante par les FAI, afin de bloquer les spam au niveau des réseaux et protéger les FAI de certains types d'attaques contre l'Internet. En ce sens, elle n'est pas aussi « intrinsèquement mauvaise » que l'estime une partie du débat public, mais elle soulève des questions éthiques importantes quand elle est mise en œuvre. Certains vendeurs ont tenté d'atténuer ces problèmes en élaborant des types de « confidentialité dès la conception » pour la DPI, bien que ces efforts en soient encore à un stade embryonnaire[105]. Dans le contexte des questions éthiques concernant le respect de la vie privée, l'inspection approfondie des paquets, en tant que technologie générique de contrôle des communications, se prête à une utilisation abusive dans de nombreux contextes différents. À mesure que l'industrie de la DPI devient mature, il reste à voir comment les différentes sociétés qui la mettent en pratique se positionneront vis-à-vis de ces utilisations abusives potentielles de la technologie de la DPI et comment la possible convergence entre différentes utilisations de la DPI a des incidences sur l'industrie dans son ensemble.

2.3.4 Omniprésence de la technologie de la géolocalisation : une nouvelle menace pour la protection de la vie privée sur l'Internet

Historiquement, les données de géolocalisation font partie intégrante de l'Internet. Les systèmes capables de localiser les internautes avec une assez grande précision sont utilisés à la fois à des fins publicitaires et à des fins juridiques. Ces services permettent de localiser géographiquement les adresses IP des internautes et permettent aux FAI d'obtenir une estimation relativement exacte du pays dans lequel se trouve un internaute et dans bien des cas de la ville où il réside. À mesure que l'utilisation de l'Internet et que les données sur l'utilisation de l'Internet ont augmenté, la précision de ces services s'est accrue et par conséquent aussi l'aptitude des sites Web et des intermédiaires à localiser géographiquement les internautes.

Toutefois, les progrès techniques des appareils connectés à l'Internet signifient que de nombreux internautes sont maintenant dotés de la technologie de localisation par GPS. Cette technologie est beaucoup plus précise, permettant de localiser un internaute à quelques mètres près. Par ailleurs, elle est incorporée dans de nombreux appareils différents et les usagers ne sont généralement pas conscients des conséquences que l'activation ou la désactivation de cette fonction peut avoir sur la protection de leur vie privée, quels programmes ou applications ont accès aux informations GPS de localisation.

La fourniture d'informations GPS est impulsée par plusieurs modèles d'affaires en ligne. Les usagers de FourSquare et de Facebook sont vivement encouragés à fournir des informations sur leur localisation quand ils visitent le site Web, avant tout à titre de fonction sociale. Cela est aussi courant dans d'autres formes de réseaux sociaux tels que « CouchSurfing », où la localisation fournie est moins précise que sur FourSquare ou Facebook. Il faut noter que ce sont tous des sites de réseaux sociaux sous une forme ou une autre, mais que pour FourSquare et CouchSurfing, on pourrait dire que la fourniture d'informations de localisation fait intrinsèquement partie du concept du réseau. Les usagers s'attendent, lorsqu'ils adhèrent à ces réseaux sociaux, à ce que leurs informations privées soient partagées et il se peut même qu'ils y adhèrent précisément pour cette raison. Cela paraît moins évident dans le cas de Facebook.

---

105 Ces considérations sont fondées sur un entretien de l'auteur de juillet 2011.

Les systèmes de géolocalisation posent clairement des problèmes pour ce qui est du consentement des usagers et de leur contrôle sur leurs données personnelles de localisation. Les usagers n'ont guère de contrôle sur les utilisateurs effectifs de leurs données et sur les formes de traitement des données qui peuvent rendre particulièrement difficile un consentement éclairé. De plus, les données de géolocalisation sont fortement traitées et peuvent – comme on l'a vu ci-dessus – être générées par d'autres informations que l'usager fournit à son insu et sans consentir à ce processus. En outre, la géolocalisation via des systèmes de GPS intégrés dans les appareils portables est aussi techniquement beaucoup plus précise que la géolocalisation des antennes de téléphonie mobile, créant une image bien plus précise des mouvements d'une personne.

Les données de localisation géographique collectées de cette manière peuvent ensuite être utilisées pour créer un profil des déplacements des individus. Un des exemples les plus évocateurs est celui de Malte Spitz, politicien allemand appartenant aux Verts, qui a poursuivi en justice son fournisseur de téléphone mobile afin d'accéder à ses données privées pour comprendre ce qu'il savait sur ses déplacements. Les données qu'il a reçues ont par la suite été visualisées par un journal allemand et elles représentent un profil complet de ses mouvements durant des mois, dont une partie a été publiée en ligne pour démontrer l'ampleur du problème[106]. Il est clair qu'alors que la technologie et les services de géolocalisation continuent de se développer massivement, il est difficile de dire quelles incidences ces développements auront sur le respect de la vie privée sur l'Internet. Pourtant, un examen attentif de certaines des questions soulevées par les informations de géolocalisation permet déjà de pronostiquer que si la géolocalisation est une question émergente, il n'y aura sans doute pas de solutions immédiates pour nombre des problèmes de confidentialité associés à la géolocalisation.

2.3.5 Traitement des données et reconnaissance faciale

« La technologie de la reconnaissance faciale est apparue comme une solution séduisante pour répondre aux nombreux besoins actuels d'identification et de vérification des revendications relatives à l'identité. Elle conjugue les promesses des autres systèmes de biométrie, qui tentent de lier l'identité à des traits corporels individuels distinctifs, et des fonctions plus familières des systèmes de surveillance visuelle »[107].

X) Retraiter les visages

Afin de démontrer les dangers associés au partage public des informations, un groupe d'artistes a téléchargé un million d'images de Facebook mises à la disposition du public, ainsi que les informations et relations personnelles qui leur étaient associées[108]. Les artistes ont ensuite utilisé ces informations pour catégoriser les visages et les (ré)assembler sur un site Web distinct. Il s'agit là d'un projet public destiné à sensibiliser à la malléabilité et à la reproductibilité

---

106 Biermann, Kai. 2011. "Data Protection: Betrayed by our own data." ZEIT Online. Extrait le 1er mars 2012 (http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz).

107 Introna, L. D., et Nissenbaum, H. F. (2009). Facial Recognition Technology: A Survey of Policy and Implementation Issues. SSRN eLibrary. SSRN.

108 Cirio, P., & Ludovico, A. (2011). Face-to-Facebook. Face-to-Facebook. Extrait de www.face-to-facebook.net/theory.php.

des données publiques, mais il existe beaucoup d'autres « bots Internet » qui passent leur temps à fouiller les sites Internet en privé et à utiliser ces informations pour alimenter des bases de données privées. Cela signifie aussi que les choix accidentels de rendre publiques des informations opérés par les internautes peuvent avoir des conséquences irréversibles, avec leurs données tirées du site Web sur lequel ils les ont rendues publiques et reproduites en une fraction de seconde. Le fait que les internautes n'ont pas conscience de la portée potentielle de leurs choix concernant la protection de leur vie privée et le manque de contrôle sur leurs propres informations une fois divulguées (pour quelque raison que ce soit) ont des effets négatifs substantiels sur la protection de la vie privée des usagers sur l'Internet.

Bien qu'il y ait eu ces dernières années des débats approfondis concernant l'impact de la technologie de la reconnaissance faciale sur la protection de la vie privée des individus, il faut situer ces débats dans un contexte plus large. Certes cette technologie comporte de nouveaux aspects du point de vue de ce débat, mais à beaucoup d'égards elle représente une nouvelle forme de traitement des données et d'identification.

Il y a beaucoup de raisons pour lesquelles les progrès du traitement des données ont des effets aussi menaçants pour la protection de la vie privée des personnes sur l'Internet. La première est que ces techniques recontextualisent les données, les traitant sous une forme qui n'était ni voulue, ni attendue, ni même concevable. Dans un contexte différent, les données traitées peuvent avoir une signification très différente. De fait, cela peut conduire à des situations dans lesquelles ceux qui traitent les données possèdent sur la vie personnelle d'un individu des informations dont l'intéressé n'a pas connaissance.

La technologie de la reconnaissance faciale sert ici à faire de ce qui était précédemment des données personnelles des informations rattachables à une personne. La puissance croissante de la technologie de la reconnaissance faciale consacre de plus en plus le visage comme identificateur unique, qui peut être relié aux profils privés et publics sur l'Internet (voir l'encadré pour plus de détails). Elle devient de plus en plus le symbole clé du lien entre les données et l'identification. En conséquence, les usagers commencent seulement à comprendre que des informations qu'ils pensaient être effectivement anonymes peuvent être associées à leur profil en ligne ou être recherchées sous leur nom. Dans un monde où le nombre de moyens de photographier augmente constamment, cela peut avoir des effets très paralysants sur la liberté d'expression et un effet également négatif sur la confidentialité[109].

109 Padania, S., Gregory, S., Alberdingk-Thijm, Y., & Nunez, B. (2011). Cameras Everywhere Report 2011. Extrait de http://www.witness.org/cameras-everywhere/report-2011.

La reconnaissance faciale est aussi utilisée par les autorités de police dans le cadre des opérations de surveillance lors de grands événements publics tels que le Superbowl de 2001 en Floride (États-Unis d'Amérique)[110]. Comme des indications similaires sont parvenues depuis lors, il y a de bonnes raisons de penser que les autorités de police et autres autorités publiques utilisent des technologies similaires de reconnaissance faciale sur l'Internet. En dépit des doutes largement partagés quant à l'efficacité de la technologie de reconnaissance faciale en tant qu'instrument d'application de la loi, le fait qu'autour du monde les autorités publiques continuent d'investir dans ces technologies donne à penser qu'elles devraient se développer rapidement dans le proche avenir[111].

Un autre fait nouveau ayant des implications substantielles pour la protection de la vie privée dans ce contexte est le transfert important de données personnelles entre le secteur public et le secteur privé. Des données personnelles qui ont été prétraitées par le secteur privé (telles qu'un profil de recherche ou un historique de la présence sur les réseaux sociaux) sont de plus en plus demandées par les autorités publiques[112]. D'autre part, des données personnelles telles que les « profils de renseignement » individuels prétraités par le secteur public sont de plus en plus communiquées au secteur privé[113]. Cette mise en commun des données personnelles traitées présente un grand risque pour le contrôle des individus sur leurs informations personnelles. Les usagers des réseaux sociaux ne s'attendent pas à ce que les données qu'ils ont entrées dans un réseau social ou les profils de leurs mouvements stockés par leur opérateur de téléphonie mobile soient communiqués à des autorités de police. Les citoyens ne s'attendent pas non plus à ce que les informations collectées par leurs services de renseignement ou leurs autorités de police soient régulièrement communiquées à des entrepreneurs privés.

La communication à double sens des informations personnelles est devenue chose courante sur l'Internet. Du reste, il semble possible de conclure à une fusion plus générale des infrastructures publiques et privées de surveillance. Les centres de fusion du renseignement, PNR, SWIFT et plus généralement les lois sur la conservation des données ne sont que quelques exemples de situations dans lesquelles des acteurs privés collectent des données qui sont ensuite utilisées par des acteurs publics et vice-versa. Ce chevauchement entre régimes publics et privés de protection de la vie privée fait qu'il est très difficile aux individus de consentir à l'utilisation de leurs données par des tiers et de savoir comment et dans quelles conditions leurs données sont stockées, sans parler de leur capacité à refuser le stockage numérique de leurs données.

Dans ce contexte, le traitement des données et la technologie de reconnaissance faciale deviennent un élément d'une plus vaste infrastructure de la surveillance qui menace fondamentalement la vie privée. La mise en place de cette infrastructure est impulsée par le désir des secteurs publics d'en savoir plus sur les citoyens, et le marché privé

---

110 Privacy International. (2006). Privacy International 2006 - Executive Summary. Extrait le 13 décembre 2011 de https://www.privacyinternational.org/article/phr2006-executive-summary.

111 Electronic Privacy Information Center. (2011). Face Recognition. (EPIC). Extrait le 13 décembre 2011 de https://epic.org/privacy/facerecognition/.

112 Google. (2011). Google Transparency Report. Google. Extrait le 13 décembre 2011 de https://www.google.com/transparencyreport/.

113 Carter, D. L., et Carter, J. G. (2009). The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement. Criminal Justice and Behavior, 36(12), 1323-1339.

qui a rapidement entrepris de répondre à cette demande[114]. En conclusion, il semble raisonnable de penser qu'il y a eu « une explosion de la diffusion d'images, dans des domaines aussi divers que le partage de photos et l'imagerie médicale, avec une augmentation correspondante du potentiel d'utilisations potentiellement intrusives de ces images. Jusqu'ici, les contrôles exercés sur les intrusions dans la vie privée que permettent ces technologies ont été très limités »[115].

2.3.6 Technologie de surveillance de l'Internet

Si l'on passe du traitement des données et de la reconnaissance faciale au marché de ces équipements, une des plus grandes menaces pour la vie privée sur l'Internet a pour origine la croissance de l'industrie de la surveillance de l'Internet. Bien que la technologie de surveillance de l'Internet soit souvent examinée dans le contexte de l'Inspection approfondie des paquets (DPI), les types de technologie utilisés dans la surveillance de l'Internet sont beaucoup plus divers. Les technologies utilisées vont des logiciels installés sur les ordinateurs individuels par les autorités de police tels que les « chevaux de Troie » et des appareils de surveillance accompagnant des systèmes informatiques ou des appareils électroniques personnels, jusqu'aux techniques de surveillance allant avec les réseaux de communications reliés à ces appareils.

Particulièrement préoccupantes du point de vue du respect de la vie privée sont les technologies de surveillance qui tentent d'exploiter les données personnelles transférées et organisées par les internautes, traitant ainsi généralement une quantité énorme d'informations personnelles. Les progrès de la puissance de traitement des ordinateurs signifient que la technologie moderne de surveillance de l'Internet est capable d'indexer, de croiser et de profiler les données personnelles des usagers. La diversité, la portée et l'utilisation des technologies de surveillance de l'Internet ont connu un développement massif depuis les débuts de l'Internet public[116]. Ces technologies sont généralement fournies aux gouvernements et aux grandes entreprises autour du monde sans qu'il soit tenu compte des utilisations abusives de la confidentialité des informations ou des autres préoccupations tenant aux droits de l'homme. Le résultat est un marché de la technologie de la surveillance sur lequel les entreprises rivalisent pour offrir les techniques les plus invasives de la vie privée. Les entreprises de ce marché n'ont guère ou nullement intérêt à protéger la vie privée des individus ; elles ont au contraire tout intérêt à supprimer la protection de la vie privée dans toute la mesure du possible.

Le commerce international de la technologie et des services de surveillance a aussi accru la transmission des données personnelles sur les réseaux de communications. La plupart des technologies modernes de surveillance sont conçues pour « téléphoner chez soi », « rapporter » ou transmettre d'une autre façon ce qu'elles ont trouvé à leurs opérateurs. Comme les opérateurs et les techniciens se trouvent rarement au même endroit que les

---

114 Silver, V., et Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. Bloomberg. Retrieved August 28, 2011, from http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

115 Senior, A., et Pankanti, S. (2011). Privacy protection and face recognition. Dans S. Z. Li & A. K. Jain (dir. pub.), Handbook of Face Recognition. Springer.

116 King, E. (2011). Our response to EU consultation on legality of exporting surveillance and censorship technology. Privacy International. Extrait le 13 décembre 2011 de https://www.privacyinternational.org/article/our-response-eu-consultation-legality-exporting-surveillance-and-censorship-technology.

équipements de surveillance, il faut que les informations personnelles collectées par les dispositifs de surveillance soient transmises par les réseaux de communications à leurs opérateurs. D'autre part, beaucoup de technologies de surveillance de l'Internet ont la capacité de se mettre à jour sur les réseaux de communications et peuvent aussi offrir un accès à distance au vendeur de la technologie de surveillance. Cette capacité d'accès à distance et la transmission de données personnelles qui lui est associée menacent à l'évidence la confidentialité des données personnelles. Il y a de nombreux cas bien documentés de technologies de surveillance compromises par des tiers (voir l'encadré pour un exemple).

De plus, l'adjonction de technologies de surveillance aux appareils techniques, systèmes et réseaux ajoute un niveau supplémentaire de vulnérabilité. Ces vulnérabilités sont d'autant plus prononcées que la technologie de surveillance est conçue pour extraire et préparer les données personnelles pour les opérateurs. En conséquence, l'accès des tiers aux systèmes de surveillance risque d'être une menace bien plus grande pour la confidentialité que l'accès aux appareils, systèmes ou réseaux étudiés. Comme on le verra plus en détail au chapitre 3, il y a un nombre limité de situations dans lesquelles l'utilisation des technologies de surveillance pourrait être justifiée dans un cadre juridique clair fondé sur les droits de l'homme et la primauté du droit. Cependant, même dans ces situations, la technologie de la surveillance est fondamentalement invasive de la vie privée, ce qui fait que son utilisation à grande échelle est extrêmement menaçante pour la confidentialité sur l'Internet.

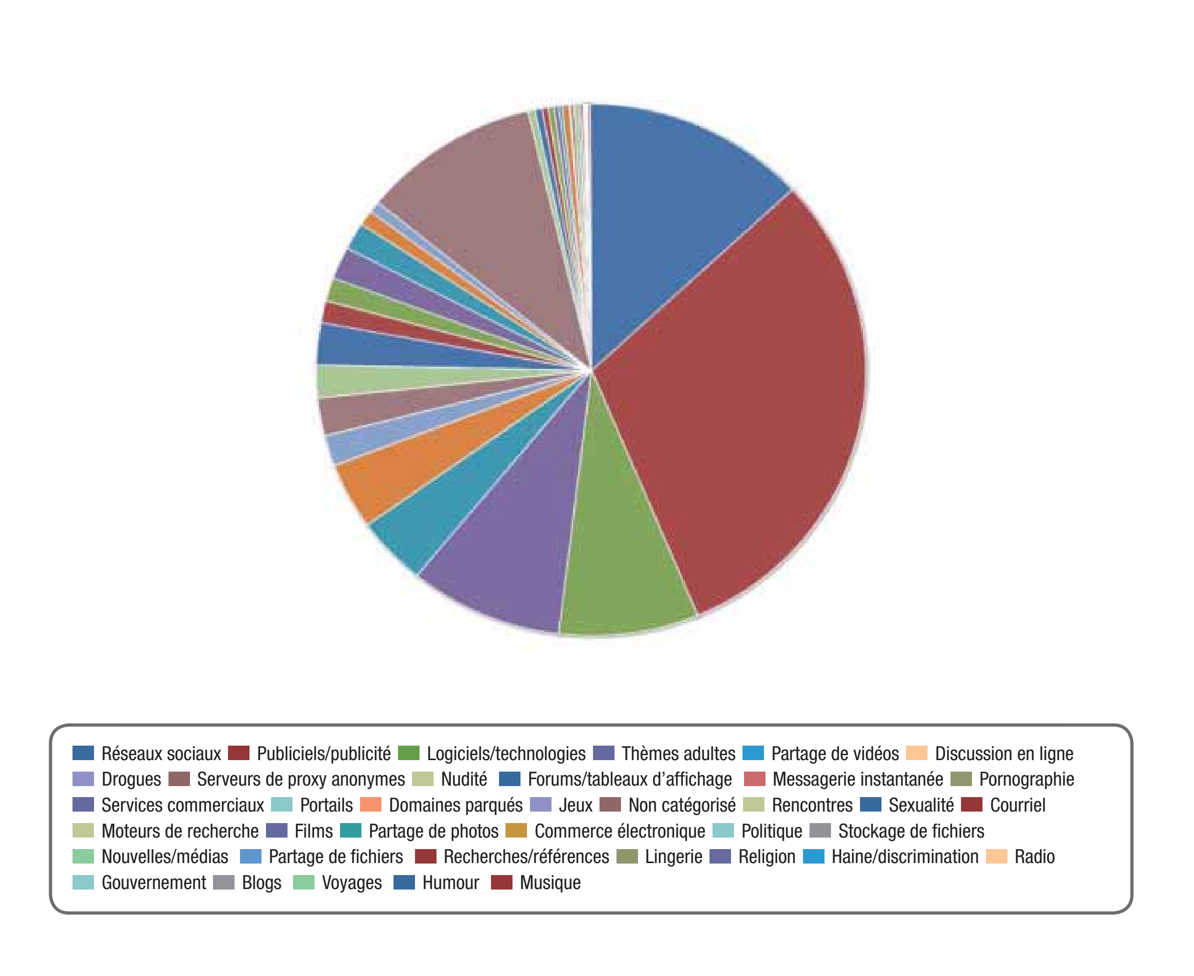
XI) Publication de journaux de surveillance

En octobre 2011, le groupe d'activistes de l'Internet Telecomix a publié quantité de fichiers journaux issus des matériels de surveillance de l'Internet en République arabe syrienne[117]. Les données de surveillance publiées offrent aussi une image extraordinaire de l'intérieur d'un système de surveillance de l'Internet. Elles donnent une idée de la façon dont les internautes ont efficacement ou vainement tenté de protéger leur vie privée et leur anonymat en utilisant les outils de l'Internet. Elles cataloguent les usagers sur les réseaux sociaux , achetant des produits, regardant des publicités, utilisant les moteurs de recherche et les sites de partage de vidéos ou de photos. Et surtout elles donnent une idée de la puissance extraordinaire des matériels de surveillance conçus pour faire intrusion dans la vie privée, au mépris de toutes les limites de l'espace privé, de l'anonymat ou de la dignité humaine. Les activités personnelles quotidiennes des individus sont décrites et cataloguées et les expressions de leurs espérances et de leurs rêves personnels, non destinées à être livrées au public, sont exposées aux regards. On pourra en trouver une brève vue d'ensemble ci-après.

117 Valentino-Devries, J., Sonne, P., et Malas, N. (2011). Blue Coat Acknowledges Syria Used Its Gear for Internet Censorship Amid Arab Spring. Wall Street Journal. Extrait le 13 décembre 2011 de http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

Figure 3 : Vue d’ensemble des journaux de surveillance[118]

Les journaux de Blue Coat indiquent les niveaux de censure en Syrie



118 Filastò, A. (2011). Blue Coat device logs indicate the levels of censorship in Syria. Extrait le 13 décembre 2011 de http://hellais.github.com/syria-censorship/.

3. ENVIRONNEMENT JURIDIQUE ET RÉGLEMENTAIRE MONDIAL DE LA PROTECTION DE LA VIE PRIVÉE

Le droit au respect de la vie privée est un droit ancien, dont les racines se trouvent dans diverses traditions religieuses – dont les traditions juive, chrétienne et musulmane – ainsi que dans la Grèce et la Chine anciennes. Certains types de protection de la vie privée existaient en Angleterre dès 1361, avec le Justices of the Peace Act qui punissait les écouteurs et regardeurs indiscrets[119]. La vie privée a été protégée en tant que droit de l'homme dès le début, étant incluse dans la Déclaration universelle des droits de l'homme (DUDH)[120] ainsi que dans le Pacte international relatif aux droits civils et politiques (PIDCP)[121].

Cependant, il s'est avéré difficile de forger un consensus sur le contenu spécifique de ce droit. Il est clair qu'il y a fondamentalement une certaine notion du droit de ne pas subir d'intrusion extérieure, mais au-delà de cette notion, divers auteurs ont proposé différentes définitions. Ainsi, le rapport du Gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord sur la vie privée, connu sous le nom de rapport Calcutt, indiquait que les auteurs n'avaient pas pu trouver une « définition entièrement satisfaisante » de la vie privée[122].

Dans leur étude fondatrice sur le sujet, en 1890, Warren et Brandeis ont défini la vie privée comme le « droit d'être laissé en paix »[123]. Des décisions judiciaires importantes aux États-Unis d'Amérique ont ensuite identifié quatre types différents d'atteintes au respect de la vie privée : l'intrusion déraisonnable dans l'intimité d'autrui, l'appropriation du nom ou de l'apparence d'autrui, la divulgation d'éléments donnant une idée fausse d'une personne et la publicité déraisonnable donnée à la vie privée d'une personne[124]. La Cour constitutionnelle d'Afrique du Sud a récemment défini le droit au respect de la vie privée comme le « droit d'une personne de vivre sa vie comme elle l'entend »[125]. La Cour suprême du Canada a défini la vie privée comme la « sphère limitée d'autonomie

---

119 Electronic Privacy Information Center and Privacy International, Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments (Electronic Privacy Information Center and Privacy International: 2007), p. 5.

120 Résolution 217A(III) de l'Assemblée générale des Nations Unies, 10 décembre 1948.

121 Adopté en vertu de la résolution 2200A(XXI) de l'Assemblée générale des Nations Unies, du 16 décembre 1966, et entré en vigueur le 23 mars 1976.

122 Calcutt, D., et al., 1990. Report of the committee on privacy and related matters, Chairman David Calcutt QC, Londres : HMSO (Cmnd. 1102), p. 7.

123 "The Right to Privacy" (1890) 4 Harvard Law Review 193, p. 195.

124 Voir Lake v. Wal-Mart-Stores Inc., 30 juillet 1998, Cour suprême du Minnesota, C7-97-263. Voir aussi Restatement (Second) of Torts, § 652B-E (1977).

125 NM and Others v. Smith and Others, 2007(7) BCLR 751, par. 33.

personnelle où se forment des choix intrinsèquement privés »[126]. La Cour européenne des droits de l'homme a évité de donner une définition, en disant : « la Cour ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de " vie privée »[127]. Dans l'affaire Ponzetti de Balbín, Indalia c. Editorial Atlàntida S.A., la Cour suprême d'Argentine s'est aussi appuyée sur une définition extrêmement large de la vie privée[128].

De plus, il est assez clair que le contenu du droit a un aspect subjectif, dans la mesure où on peut, en traitant quelque chose comme public par nature, le rendre effectivement tel, ou peut-être céder une partie de sa vie privée. Ainsi, l'orientation sexuelle d'une personne est privée, mais on peut la changer en la rendant publique de façon répétée, par le plaidoyer. À cet égard, ce droit peut être mis en opposition avec d'autres droits de la personne tels que le droit à la réputation ou à la liberté d'expression, dont les limites sont beaucoup plus claires et objectives. On peut ainsi le rapprocher de la pornographie, dont le juge Stewart de la Cour suprême des États-Unis notait qu'il était difficile de la définir « mais je la reconnais quand je la vois »[129]. Le problème de la définition est rendu encore plus complexe par le rôle de la notion d'intérêt public, également difficile à définir comme chacun sait, pour définir la portée de la protection de la vie privée. L'absence de définition claire a contribué aux difficultés rencontrées pour appliquer et faire respecter le droit à la protection de la vie privée.

L'idée de protection des données, qui est particulièrement pertinente par rapport au concept de vie privée et à l'Internet, est d'origine bien plus récente, car sa genèse se trouve essentiellement dans la collecte croissante par les gouvernements de données personnelles sur les individus. L'arrivée des ordinateurs et ensuite de l'Internet a considérablement favorisé l'élaboration du concept de protection des données. La toute première loi sur la protection des données a été attribuée au Land de Hesse en Allemagne en 1970, et la Suède est considérée comme le premier pays à avoir adopté une loi nationale, en 1973.

Le concept de base de la protection des données est que les individus ont le droit de contrôler la collecte et l'utilisation des données permettant de les identifier (données personnelles). Comme la protection de la vie privée, la protection des données est assujettie à certaines contraintes, dont une des plus évidentes est celle des enquêtes de police sur les crimes et délits. La protection des données contraste avec celle de la vie privée dans la mesure où ses concepts de base sont assez clairs et consensuels, quoique avec quelques variations importantes.

---

126 Godbout c. Longueuil (Ville) [1997] 3 RCS 844, par. 97.

127 Niemietz c. Allemagne, 16 décembre 1992, 16 EHRR 97, par. 29. Voir aussi Workman, R., qui a écrit en 1992 : « Une définition solide de la « vie privée » n'a pas pu être trouvée par les commentateurs ». "Balancing the Right to Privacy and the First Amendment" (1992) 29 Houston Law Review 1059, p. 1063.

128 Décision datée du 11 décembre 1984. Corte Suprema de Justicia de la Nación (CS), par. 8. Disponible à l'adresse http://www.fallodelderecho.com.ar/jurisprudencia-argentina/ponzetti-de-balbin.

129 Jacobellis v. Ohio, 378 U.S. 184 (1964), at. 197.

Une question importante pour la confidentialité sur l'Internet en général est la relation précise entre la protection de la vie privée et la protection des données ou, autrement dit, la mesure dans laquelle les principes de la protection des données trouvent une justification dans le cadre du droit établi de la personne humaine à la protection de sa vie privée. Il est clair que les deux questions sont différentes et que la protection des données n'est pas entièrement couverte par le concept de protection de la vie privée[130]. Toutefois, on peut tirer directement du droit de la personne humaine au respect de sa vie privée des principes importants pour la protection des données, ce que confirme la jurisprudence internationale. Cela est moins clair pour les autres principes et certainement pour les systèmes qui sont utilisés pour assurer concrètement la protection des données.

3.1 Protection internationale de la vie privée et des données personnelles

3.1.1 Vie privée

3.1.1.1 Normes mondiales

La vie privée est directement et explicitement protégée par le régime international des droits de l'homme. L'article 12 de la DUDH dispose :

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

La protection juridique de ce droit a été officialisée par l'article 17 du Pacte international relatif aux droits civils et politiques, qui dispose :

(1) Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

(2) Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Ces deux définitions sont similaires, bien qu'avec d'importantes différences. La DUDH ne protège que contre les immixtions arbitraires, mais non illégales, dans la vie privée. En pratique, cela n'a sans doute qu'une importance limitée, car une immixtion illégale sera toujours arbitraire. Dans la mesure où il s'agit d'honneur et de réputation, le Pacte ne protège que contre les atteintes illégales, tandis que la Déclaration protège contre toutes les atteintes. La différence est peut-être plus conséquente par nature, mais elle n'a pas été testée par la jurisprudence.

---

130 C'est pourquoi la Charte des droits fondamentaux de l'Union européenne protège à la fois la vie privée et les données (voir note 208). Les nouvelles propositions de la Commission européenne pour la réglementation de la protection des données reflètent aussi cette idée, en disant : « La protection des données est étroitement liée au respect de la vie privée et familiale ». Note 217, p. 7.

Le Comité des droits de l'homme de l'ONU a dit clairement dans son Observation générale sur l'article 17 que la protection du droit au respect de la vie privée doit être garantie « contre toutes ces immixtions et atteintes, qu'elles émanent des pouvoirs publics ou de personnes physiques ou morales »[131]. L'Observation générale du Comité ne fournit néanmoins guère d'indications sur la signification des mots « arbitraires » et « vie privée ». Concernant la notion d'arbitraire, le Comité a estimé qu'une immixtion prévue par la loi pouvait être arbitraire et que toute immixtion prévue par la loi devait être « conforme aux dispositions, aux buts et aux objectifs du Pacte et […], dans tous les cas, raisonnable eu égard aux circonstances particulières »[132]. En définitive, cela donne très peu d'indications sur ce qui peut être considéré comme « arbitraire », bien que cela interdise au moins les immixtions dans la vie privée prévues par des lois contraires aux buts du Pacte ou déraisonnables.

L'Observation générale contient aussi des remarques assez développées, quoique générales, sur la protection des données, disant que le rassemblement et la conservation d'informations personnelles par des autorités publiques ou des organismes privés doivent être réglementés, et que les individus ont le droit de déterminer quelles informations sont détenues à son sujet, à quelles fins et par qui[133].

La jurisprudence du Comité dans ce domaine est aussi limitée. Dans l'affaire Hulst c. Pays-Bas, le Comité a dû déterminer si l'interception des appels téléphoniques de l'auteur, un avocat, qui avaient été utilisés pour le déclarer coupable d'un crime, représentait une intrusion injustifiée dans sa vie privée. En statuant qu'il n'y avait pas eu d'immixtion, le Comité a cité les normes notées ci-dessus dans son Observation générale et jugé que l'immixtion était autorisée par la loi et raisonnable[134].

3.1.1.2 Système africain et système interaméricain

Il n'y a pas de protection explicite de la vie privée dans la Charte africaine des droits de l'homme et des peuples[135]. La protection de la vie privée est prévue dans la Convention américaine relative aux droits de l'homme[136] à son article 11 et dans la Convention européenne des droits de l'homme[137] à son article 8.

Les dispositions pertinentes de la Convention américaine sont les suivantes :

> (2) Nul ne peut faire l'objet d'ingérences arbitraires ou abusives dans sa vie privée, dans la vie de sa famille, dans son domicile ou sa correspondance, ni d'attaques illégales à son honneur et à sa réputation.
>
> (3) Toute personne a droit à la protection de la loi contre de telles ingérences ou de telles attaques.

---

131 Observation générale n° 16 : Article 17 (Droit au respect de la vie privée), adoptée le 4 août 1988, par. 1.
132 Ibid., par. 4.
133 Ibid., par. 10.
134 Communication n° 903/1999, 1er novembre 2004.
135 Adoptée le 26 juin 1981, document OUA CAB/LEG/67/3 rev. 5, 21 I.L.M. (1982), entrée en vigueur le 21 octobre 1986.
136 Adoptée le 22 novembre 1969, OAS Treaty Series n° 36, entrée en vigueur le 18 juillet 1978.
137 Adoptée le 4 novembre 1950, ETS n° 5, entrée en vigueur le 3 septembre 1953.

Ces dispositions sont très similaires à celles qu'on trouve dans la DUDH et le PIDCP. Il n'y a guère de jurisprudence de la Cour interaméricaine des droits de l'homme traitant directement de cette question. Une récente affaire importante sur la vie privée, jugée en novembre 2011, est Fontevecchia & D'Amico c. Argentine[138]. Dans cette affaire, la Cour interaméricaine a statué que la publication de certaines informations privées sur Menem, ex-président de l'Argentine, n'était pas une ingérence dans sa vie privée, pour les motifs que ces informations étaient déjà bien connues, qu'elles n'avaient pas été traitées confidentiellement par Menem et qu'elles présentaient un intérêt public considérable.

La Cour interaméricaine a traité de la vie privée dans un certain nombre d'autres occasions. Dans l'affaire Tristán Donoso c. Panama, la Cour a conclu à une atteinte à la vie privée lorsque des agents de l'État ont diffusé un enregistrement d'une conversation téléphonique privée apparemment échangée entre une partie privée et des dignitaires religieux ainsi que des membres du Barreau[139]. Dans l'affaire Escher et al. c. Brésil, la Cour a émis plusieurs conclusions importantes concernant la protection de la vie privée dans le contexte de la surveillance téléphonique. Tout d'abord, elle a statué que si la charge de la preuve des faits d'une violation des droits de l'homme incombait normalement au plaignant, il était légitime de tirer des conclusions raisonnables lorsqu'il était impossible au plaignant de prouver ces faits de manière concluante en raison du secret imposé par l'État[140]. Etant donné la nature intrusive de l'interception téléphonique, la Cour a statué :

Cette mesure doit être fondée sur une loi qui doit être précise et indiquer les règles claires et détaillées à appliquer, telles que les circonstances dans lesquelles cette mesure peut être prise, les personnes habilitées à la demander, à l'ordonner et à l'exécuter, et la procédure à suivre[141].

Dans cette affaire, les règles n'avaient pas été appliquées de façon appropriée, et en conséquence l'ingérence dans la vie privée ne satisfaisait pas à l'exigence de légalité comme stipulé dans la Convention interaméricaine[142]. La divulgation de certains des matériels privés par des agents de l'État représentait une autre atteinte au droit au respect de la vie privée[143].

Pour ce qui est de la protection des données, la Commission interaméricaine a indiqué clairement qu'elle estime qu'il existe un droit d'habeas data en vertu de la Convention interaméricaine, qui confère aux individus le droit de savoir quelles informations l'État et les acteurs privés ont collectées à leur sujet, d'y accéder et de les modifier, rectifier ou supprimer, en tant que de besoin[144]. La Cour interaméricaine n'a jamais directement examiné la question du droit d'habeas data.

---

138 29 novembre 2011, Series C, n° 238.
139 27 janvier 2009, Series C, n° 193, par. 83.
140 6 juillet 2009, Series C, n° 200, par. 127-128.
141 Ibid., par. 131.
142 Ibid., par. 146.
143 Ibid., par. 164.
144 Commission interaméricaine des droits de l'homme, Report on the Situation of Human Rights Defenders in the Americas, par. 89. Disponible à l'adresse http://www.cidh.org/countryrep/defenders/defenderschap1-4.htm.

3.1.1.3 Convention européenne des droits de l'homme : vue d'ensemble

L'article 8 de la Convention européenne des droits de l'homme formule le droit au respect de la vie privée en des termes assez différents de ceux qu'emploient le Pacte international relatif aux droits civils et politiques ou la Convention américaine des droits de l'homme :

> (1) Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> (2) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

La caractérisation du droit est ici plus positive ; il s'agit plutôt d'un droit au respect de sa vie privée que d'un droit d'être protégé contre les ingérences. Une autre différence est que la protection se limite aux ingérences des autorités publiques, bien que la Cour européenne des droits de l'homme n'ait pas interprété cette disposition de façon aussi restrictive (voir ci-dessous). Enfin, les normes applicables aux limitations sont énoncées beaucoup plus clairement. Au lieu de termes vagues tels qu'« arbitraire », « illégal » et « abusif », nous avons affaire à un test clair à trois volets : (a) conformément à la loi ; (b) nécessaire dans une société démocratique et (c) visant à protéger un des intérêts énumérés (sécurité nationale, ordre public, etc.).

Quant à la portée de la notion de vie privée, la Cour européenne a identifié un certain nombre de types spécifiques d'actions de l'État qui peuvent porter atteinte au droit, comme l'interception des communications privées ou les écoutes téléphoniques, quel que soit le contenu de la communication[145], l'attribution des droits sur les enfants[146], les immixtions dans la vie sexuelle[147], le traitement médical forcé[148] et l'accès à certains types d'informations détenues par l'État[149]. La Cour s'est abstenue de proposer une définition générique de la vie privée, estimant au contraire, comme on l'a noté précédemment, que ce n'est pas possible[150].

La Cour a néanmoins indiqué un certain nombre de caractéristiques du droit. Dans l'affaire Von Hannover c. Allemagne, par exemple, la Cour a statué que la notion de vie privée comprend « des éléments se rapportant à l'identité d'une personne tels que son

---

145 Voir par exemple Lordachi et autres c. Moldova, 10 février 2009, Requête n° 25198/02. Voir aussi Halford c. Royaume-Uni, 25 juin 1997, Requête n° 20605/92, par. 44.

146 Voir par exemple Elsholz c. Allemagne, 13 juillet 2000, Requête n° 25735/94.

147 Voir par exemple Dudgeon c. Royaume-Uni, 22 octobre 1981, Requête n° 7525/76. Voir aussi Mosley c. Royaume-Uni, 10 mai 2011, Requête n° 48009/08.

148 Voir par exemple Acmanne et autres c. Belgique, 10 décembre 1984, Décision sur la recevabilité, Requête n° 10435/83.

149 Voir par exemple Gaskin c. Royaume-Uni, note 167.

150 Voir Niemietz c. Allemagne, note 127. Dans l'affaire Costello-Roberts c. Royaume-Uni, la Cour a estimé que la notion de vie privée « ne se prête pas à une définition exhaustive ». 25 mars 1993. Requête n° 13134/87, par. 36. L'affaire concernait un châtiment corporel dans une école privée qui, de l'avis de la Cour, ne portait pas atteinte à la vie privée compte tenu des circonstances.

nom ou son droit à l'image ». De plus, le droit est destiné à « assurer le développement, sans ingérences extérieures, de la personnalité de chaque individu dans ses relations avec ses semblables »[151]. Dans l'affaire Niemietz c. Allemagne, elle avait statué que « il serait […] trop restrictif de limiter [la notion de vie privée] à un « cercle intime » où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables »[152]. Les relations commerciales et professionnelles entraient dans le cadre de ce concept, si bien que la recherche de locaux commerciaux représentait une ingérence dans la vie privée[153].

La Cour a noté que « ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un élément significatif, quoique pas nécessairement décisif »[154]. Même des informations recueillies dans des situations publiques peuvent, par l'utilisation à laquelle elles peuvent donner lieu, soulever des questions tenant à la vie privée. Ainsi, « la création d'un enregistrement systématique ou permanent de tels éléments appartenant au domaine public peut donner lieu à des considérations liées à la vie privée »[155].

En pratique, la Cour a eu tendance à reconnaître au droit une assez large portée, tout en reconnaissant aussi la possibilité de restrictions, ainsi qu'une large marge d'appréciation des États, en particulier dans les affaires impliquant la protection des enfants. Par exemple, dans l'affaire Keegan c. Irlande, la Cour a déclaré que les États « jouissent d'une large marge d'appréciation en matière d'adoption »[156]. L'affaire concernait un père qui cherchait à obtenir la garde de son enfant, que la mère de celui-ci, ayant rompu avec le père, proposait à l'adoption. Dans l'affaire Von Hannover c. Allemagne (n° 2), qui portait sur la publication de photos présentées comme privées, la Cour a statué : « Les États contractants disposent d'une certaine marge d'appréciation pour juger de la nécessité et de l'ampleur d'une ingérence dans la liberté d'expression protégée par cette disposition »[157].

3.1.1.4 Convention européenne des droits de l'homme : restrictions

La Cour a élaboré une méthodologie assez claire pour appliquer le triple test des restrictions dans les affaires impliquant des ingérences dans la vie privée. Dans un certain nombre d'affaires, concernant surtout les écoutes téléphoniques et autres formes de surveillance, la Cour a noté qu'en raison de la nature particulièrement invasive de ces activités, celles-ci doivent « se fonder sur une « loi » d'une précision particulière… d'autant que les procédés techniques utilisables ne cessent de se perfectionner »[158].

---

151 24 juin 2004, Requête n° 59320/00. Les références aux autres décisions judiciaires et textes ont été supprimées ici et dans les autres citations du texte.
152 16 décembre 1992, Requête n° 13710/88, par. 29.
153 Voir aussi Von Hannover c. Allemagne (n° 2), 7 février 2012, Requêtes n° 40660/08 et 60641/08, par. 95.
154 P.G. et J.H. c. Royaume-Uni, 25 septembre 2001. Requête n° 44787/98, par. 57.
155 Ibid. Par exemple, les informations collectées ouvertement par des services de sécurité peuvent être couvertes. Voir Rotaru c. Roumanie, 4 mai 2000, Requête n° 28641/95.
156 26 mai 1994, Requête n° 16969/90, par. 47. D ns
157 Note 153, par. 104.
158 Voir par exemple Kruslin c. France, 24 avril 1990, Requête n° 11801/85, par. 33. Voir aussi Rotaru c. Roumanie, note 155, par. 62. Cette dernière affaire concerne la collecte de données personnelles.

Dans l'affaire Kruslin c. France, la Cour a statué que cette condition n'était pas remplie parce que les conditions auxquelles étaient subordonnées les écoutes téléphoniques n'étaient pas assez précises. Rien ne précisait, en particulier, les catégories de personnes susceptibles d'être mises sous écoute judiciaire, rien n'astreignait le juge à fixer une limite à la durée de l'exécution de la mesure, rien ne précisait les conditions d'établissement des procès-verbaux d'enregistrement des conversations interceptées ni les procédures de destruction des enregistrements ou les précautions à prendre pour garder intacts les enregistrements[159].

Dans l'affaire Malone c. Royaume-Uni, la Cour européenne a examiné la pratique consistant à compter les appels téléphoniques (c'est-à-dire à enregistrer les numéros appelés et la durée des appels). Elle a distingué cette pratique de l'interception effective des appels, mais a noté que si cette pratique était légitime (sur la base du consentement présumé) aux fins de facturation et de contrôle de la bonne utilisation du service, la transmission de ces informations à la police représentait une ingérence dans la vie privée. Aucune loi n'imposait au Post Office (organisme public qui était devenu les British Telecommunications au moment de l'affaire), qui procédait au comptage, de transmettre les enregistrements à la police, mais en pratique le Post Office le faisait lorsque la police avait vraiment besoin de ces renseignements « pour ses enquêtes concernant des infractions graves » et ne pouvait « les recueillir à une autre source ». Cette pratique ne satisfaisait pas au critère selon laquelle elle devait être « prévue par la loi » au sens de l'article 8(2) de la Convention[160]. Cela vaut clairement pour d'autres affaires dans lesquelles des acteurs privés – tels que les fournisseurs d'accès à l'Internet – collaborent avec des organismes publics dans des domaines qui ont un impact sur les droits au respect de la vie privée.

Pour ce qui est du deuxième volet du test, en général, la Cour n'a pas de problème pour reconnaître un but légitime qu'il faut protéger dans les affaires de respect de la vie privée, à savoir souvent les droits d'autrui ou l'ordre public. Ainsi, dans l'affaire Leander c. Suède, la Cour a statué dans un bref paragraphe qu'une loi autorisant la police à tenir secrètes les informations recueillies sur les candidats à certains emplois était nécessaire pour protéger la sécurité nationale[161], tandis que dans l'affaire Murray c. Royaume-Uni, la Cour a de même consacré un seul paragraphe à la reconnaissance de la prévention de la délinquance comme but légitime[162].

En évaluant l'aspect nécessité du test, la Cour a déclaré : « Il faut avoir égard au juste équilibre à ménager entre les intérêts concurrents de l'individu et de la société dans son ensemble »[163]. De plus, « la notion de nécessité implique une ingérence fondée sur un besoin social impérieux et notamment proportionnée au but légitime recherché » et il faut déterminer si « les motifs invoqués à l'appui des ingérences sont « pertinents et suffisants »[164]. Comme les tribunaux nationaux, la Cour européenne s'est appuyée sur l'idée de l'intérêt général pour évaluer les restrictions apportées à la protection de la vie privée, en particulier lorsque des droits de l'homme concurrents sont en jeu, comme il ressort clairement de l'encadré consacré ci-dessous à l'affaire Von Hannover.

---

159 Ibid., Kruslin c. France, par. 35.
160 Malone c. Royaume-Uni, 2 août 1984, Requête n° 8691/79, par. 83-86.
161 26 mars 1987, Requête n° 9248/79, par. 49.
162 28 octobre 1994, Requête n° 14310/83, par. 89.
163 Keegan c. Irlande, note 156, par. 49.
164 Olsson c. Suède, 24 mars 1988, Requête n° 10465/83, par. 67-68.

3.1.1.5 Convention européenne des droits de l'homme : acteurs privés

La Cour européenne a en plusieurs occasions abordé la question des ingérences dans la vie privée imputables à des intérêts privés. Elle a souligné que « [l'article 8] a « essentiellement » pour objet de prémunir l'individu contre des ingérences arbitraires des pouvoirs publics »[165]. La Cour a reconnu que des intérêts privés peuvent imposer aux États des obligations positives d'agir pour préserver la vie privée. Elle utilise parfois les obligations positives dans des affaires où ce n'est pas que l'État ait agi mais qu'il s'est abstenu d'agir pour protéger la vie privée[166]. Certaines de ces affaires ont trait à la relation entre les individus et l'État, soit à l'application « verticale » des droits. Gaskin c. Royaume-Uni en est un exemple. Dans cette affaire, la Cour a estimé qu'une autorité publique était tenue de divulguer certaines informations personnelles relatives au demandeur pour protéger un intérêt au respect de la vie privée[167].

D'autre part, la Cour s'est dans certaines affaires référée à l'obligation positive des États de réglementer les relations entre les acteurs non étatiques, à savoir l'application « horizontale » des droits. Dans ces affaires, ce n'est pas la relation entre l'État et un individu – soit en raison d'une mesure que l'État a prise soit en raison de l'inaction de l'État – qui est en question. C'est l'assertion selon laquelle la protection effective de la vie privée exige que l'État réglemente les relations entre les acteurs non étatiques, par exemple en prévoyant des voies de recours contre les immixtions dans la vie privée.

Dans certaines de ces affaires, il y a eu un élément de participation de l'État à l'atteinte à la vie privée. Par exemple, dans l'affaire López Ostra c. Espagne, la Cour a jugé que l'absence d'action des autorités pour prévenir les effets préjudiciables d'une grave pollution environnementale due à une station d'épuration violait l'article 8. Toutefois, la Cour a noté expressément que la légalité de la station au regard de la loi espagnole était en question et s'est concentrée sur le fait que les autorités non seulement n'avaient pas protégé Mme López Ostra mais avaient contribué à prolonger la situation[168]. Dans l'affaire X et Y c. Pays-Bas[169], la Cour a estimé qu'un recours civil ne suffisait pas pour protéger les individus contre les agressions sexuelles et qu'il faudrait un recours pénal. Les Pays-Bas offraient normalement un recours pénal en cas d'agression sexuelle ; cela n'était pas applicable en l'occurrence, en raison de certaines questions de procédure en rapport avec le fait que la victime était mentalement handicapée.

Cependant, dans d'autres affaires, la Cour a estimé que les États portaient atteinte au droit à la protection de la vie privée dans des cas concernant des actions entre parties privées (voir encadré).

XII) Les affaires Von Hannover c. Allemagne

Deux décisions rendues en 2004 et 2012 par la Cour européenne des droits de l'homme, Von Hannover c. Allemagne et Von Hannover c. Allemagne (n° 2) énoncent des règles claires concernant le respect de la vie privée. La première

165 Voir Marckx c. Belgique, 13 juin 1979, Requête n° 6833/74, par. 31.
166 Airey c. Irlande, 9 octobre 1979, Requête n° 6289/73, par. 37.
167 Gaskin c. Royaume-Uni, 7 juillet 1989, Requête n° 10454/83, par. 41 et 49.
168 9 décembre 1994, Requête n° 16798/90, par. 54-56.
169 26 mars 1985, Requête n° 8978/80.

affaire concernait un certain nombre de photos de la princesse Caroline de Monaco montant à cheval, en train de skier et trébuchant sur un obstacle sur une plage privée. Les photos avaient été publiées dans des magazines privés en Allemagne et l'affaire portait donc sur l'application horizontale des droits. Les tribunaux allemands ont pour l'essentiel soutenu la publication des images (à l'exception de certaines photos prises dans des endroits où la princesse pouvait raisonnablement compter sur le respect de sa vie privée et de quelques images comportant ses enfants).

La situation était dans une large mesure identique dans la deuxième affaire si ce n'est que les photos en question concernaient pour la plupart la question de la maladie du prince régnant de Monaco, le prince Rainier, et la façon dont sa famille s'était occupée de lui durant cette maladie.

Dans la première affaire, la Cour européenne a statué :

> Dans les affaires relatives à la mise en balance de la protection de la vie privée et de la liberté d'expression dont la Cour a eu à connaître, elle a toujours mis l'accent sur la contribution que la parution de photos ou d'articles dans la presse apportait au débat d'intérêt général[170].

La Cour a aussi fait observer :

> La Cour considère qu'il convient d'opérer une distinction fondamentale entre un reportage relatant des faits – même controversés – susceptibles de contribuer à un débat dans une société démocratique, se rapportant à des personnalités politiques, dans l'exercice de leurs fonctions officielles par exemple, et un reportage sur les détails de la vie privée d'une personne qui, de surcroît, comme en l'espèce, ne remplit pas de telles fonctions[171].

Les tribunaux allemands avaient considéré que la princesse Caroline était une figure de la société contemporaine « par excellence » et qu'elle n'avait donc pas de droit au respect de sa vie privée à moins qu'elle ne soit retirée dans un endroit isolé à l'abri des regards indiscrets. La Cour européenne a estimé que cette position pouvait être appropriée dans le cas de politiciens exerçant des fonctions officielles mais n'était pas justifiée en l'occurrence. Comme la Cour l'a noté à propos de la requérante, « l'intérêt du grand public et de la presse est fondé uniquement sur son appartenance à une famille régnante, alors qu'elle-même ne remplit pas de fonctions officielles »[172].

Dans la deuxième affaire, la Cour a énoncé un certain nombre de critères à prendre en compte pour ménager l'équilibre entre la liberté d'expression et la protection de la vie privée :

- la contribution à un débat d'intérêt général (par. 109) ;
- la notoriété de la personne visée et l'objet du reportage (par. 110) ;
- le comportement antérieur de la personne concernée (par. 111) ;
- le contenu, la forme et les répercussions de la publication (par. 112) ; et
- les circonstances de la prise des photos (par. 113).

---

170 Note 151, par. 60.
171 Ibid., par. 63.
172 Ibid., par. 72.

D'une façon générale, la Cour a paru disposée à autoriser une grande latitude, même pour les photos, lorsqu'il y a une contribution à un débat d'intérêt général. L'absence complète de pareille contribution dans la première affaire – dont la meilleure illustration est sans doute la photo de la princesse Caroline trébuchant sur un obstacle sur la plage – a dicté la conclusion particulière à laquelle la Cour est parvenue, tandis que dans la deuxième affaire, la Cour a estimé que « les articles rendaient compte aussi de la maladie du prince Rainier III, souverain régnant de la principauté de Monaco à l'époque, et du comportement des membres de sa famille pendant cette maladie » et portaient donc sur une question d'intérêt général[173].

3.1.1.6 Convention européenne des droits de l'homme : protection des données

La Cour n'a jamais reconnu de droit général à la protection des données en vertu de l'article 8 de la Convention, du moins dans l'acception courante de cette expression. Toutefois, dans une série d'affaires, elle a reconnu divers éléments des droits généralement associés à la protection des données.

Tout d'abord, dans un certain nombre de décisions, la Cour a statué que la collecte d'informations privées suscite une préoccupation pour le respect de la vie privée. Par exemple, dans l'affaire Murray c. Royaume-Uni, le gouvernement ne contestait pas et la Cour a admis que la collecte d'informations personnelles (dont une photo) lors de l'arrestation représentait une ingérence dans la vie privée, bien que justifiée en tant que limitation de ce droit dans les circonstances de l'affaire[174].

Dans l'affaire Leander c. Suède, la Cour a statué que le stockage et la divulgation d'informations relatives à la vie privée représentaient une ingérence dans la vie privée[175]. Dans cette affaire, la Cour a examiné de façon assez détaillée les garanties procédurales requises pour que la collecte des informations – en l'occurrence pour déterminer l'aptitude à être employé dans un musée naval – réponde à l'exigence de la nécessité dans une société démocratique. La Cour a admis qu'il puisse être nécessaire de recueillir ce type d'informations pour protéger la sécurité nationale, mais elle a estimé qu'il fallait des « garanties adéquates et suffisantes contre les abus »[176]. Elle a noté que la loi pertinente contenait des dispositions visant à réduire au strict minimum l'utilisation des informations, en particulier dans les autres domaines que le contrôle du personnel où elles ne peuvent servir que dans les poursuites pénales et les affaires de naturalisation. La Cour a dit attacher un grand prix à la fonction de supervision du système confiée à des acteurs extérieurs tels que les parlementaires, le Chancelier de la justice, le médiateur parlementaire et la Commission parlementaire de la justice.

Deuxièmement, la Cour a statué que la diffusion d'informations privées par des organismes publics suscite une préoccupation pour le respect de la vie privée. Dans l'affaire Z. c. Finlande, la question était celle de la divulgation de certaines informations sur la requérante, dont sa séropositivité, dans le cadre du processus judiciaire. La Cour n'a pas hésité à décider que c'était là une ingérence dans le droit de la requérante au respect de sa vie privée. De fait, la Cour a statué que la protection de ces données personnelles,

173 Note 153, par. 117.
174 Note 162, par. 86.
175 Note 161. Voir aussi Rotaru c. Roumanie, note 158.
176 Ibid., par. 60.

et en particulier des informations relatives à la santé de la requérante, jouait un « rôle fondamental … pour l'exercice du droit au respect de la vie privée et familiale »[177]. Étant donné le caractère particulièrement sensible des renseignements médicaux en question, « toute mesure prise par un État pour contraindre à communiquer et à divulguer pareil renseignement sans le consentement de la personne concernée appelle un examen des plus rigoureux de la part de la Cour, qui doit apprécier avec un soin égal les garanties visant à assurer une protection efficace »[178]. En acceptant la divulgation de certains renseignements sur une base limitée, la Cour a souligné le fait que la requérante avait bénéficié de possibilités adéquates de contester les divulgations et l'importance des renseignements en tant qu'éléments de preuve dans une affaire pénale grave[179]. La Cour a cependant indiqué que la divulgation publique des informations au terme d'un délai de dix ans, ainsi que leur divulgation dans l'arrêt de la Cour d'appel, alors que d'autres options étaient disponibles (telles que l'omission du nom de la requérante), constituaient des atteintes au droit au respect de la vie privée[180].

Même les divulgations internes (à savoir les divulgations au sein du secteur public) soulèvent des questions de respect de la vie privée. L'affaire M. S. c. Suède concernait la divulgation de certains renseignements médicaux par un hôpital public à la Caisse de sécurité sociale, dans le contexte d'une demande présentée à la Caisse en vue d'obtenir des prestations afférentes à l'état de santé de la requérante. Il n'était pas contesté que cette affaire concernait des questions en rapport avec la vie privée. La Cour a rejeté l'assertion du gouvernement selon laquelle en présentant sa demande, la requérante avait consenti à la divulgation, en partie parce que l'étendue de la divulgation n'avait pas été déterminée par elle[181]. En statuant que l'ingérence était justifiée, la Cour a noté que la Caisse avait besoin d'accéder à ces renseignements pour évaluer la demande d'indemnisation et souligné la nécessité de fortes garanties de la confidentialité, telles que des sanctions sévères contre les divulgations faites hors du strict cadre de la loi[182].

Troisièmement, dans un certain nombre d'affaires – dont Leander c. Suède[183], Gaskin c. Royaume-Uni[184], Guerra et autres c. Italie[185], McGinley et Egan c. Royaume-Uni[186], Odièvre c. France[187] et Roche c. Royaume-Uni[188] – la Cour a affirmé un droit des individus à accéder aux informations les concernant détenues par des autorités publiques. Dans chacune de ces affaires, la Cour a conclu que le refus de donner accès aux informations en question était une ingérence dans le droit au respect de la vie privée et/ou familiale, en admettant toutefois que le refus d'accès pouvait constituer une limitation légitime de ces droits.

---

177 25 février 1997, Requête n° 22009/93, par. 94.
178 Ibid., par. 96.
179 Ibid., par. 101-109.
180 Ibid., par. 111-113. Voir aussi Rotaru c. Roumanie, note 158.
181 22 août 1997, Requête n° 20837/92, par. 35.
182 Ibid., par. 42-43.
183 Note 175.
184 7 juillet 1989, Requête n° 10454/83, 12 EHRR 36.
185 19 février 1998, Requête n° 14967/89.
186 9 juin 1998, Requête n° 21825/93 et 23414/94.
187 13 février 2003, Requête n° 42326/98.
188 19 octobre 2005, Requête n° 32555/96.

XIII) Affaires soumises à la Cour européenne des droits de l'homme sur l'accès aux informations privées

Dans la première affaire sur l'accès aux informations privées dont a été saisie la Cour européenne, Leander, le requérant, avait été licencié pour des raisons de sécurité alors qu'il occupait un emploi au service du Gouvernement suédois mais s'était vu refuser l'accès aux informations sur sa vie privée, conservées dans un registre secret de la police, qui avaient servi de base à son licenciement. La Cour a statué que le stockage et l'utilisation des informations, associées au refus d'offrir au requérant la possibilité de les réfuter, constituaient une ingérence dans son droit au respect de la vie privée. L'ingérence était néanmoins justifiée en tant que nécessaire pour protéger la sécurité nationale de la Suède[189]. Il est intéressant de noter qu'en définitive il est apparu que Leander avait en fait été licencié pour ses convictions politiques, et que le Gouvernement suédois lui a présenté ses excuses et offert une indemnisation.

Dans l'affaire *Gaskin*, le requérant, qui lorsqu'il était enfant avait été pris en charge par les autorités locales au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, avait demandé vainement la permission d'accéder au dossier le concernant détenu par l'État. La Cour a statué que le requérant avait le droit de recevoir les informations nécessaires pour connaître et comprendre son enfance et ses années de formation, bien qu'il faille équilibrer ce souci avec la confidentialité due aux tiers qui avaient fourni les informations. Cela imposait au gouvernement une obligation positive de charger un organe indépendant de décider s'il y avait lieu d'accorder l'accès si un tiers informateur n'était pas disponible ou refusait la divulgation. Etant donné que le gouvernement n'avait pas pris ces dispositions, les droits du requérant avaient été bafoués[190].

Dans l'affaire *Guerra*, les requérantes, qui vivaient près d'une usine chimique « à haut risque », se plaignaient que les autorités locales italiennes ne leur avaient pas fourni d'informations sur les risques de pollution et sur ce qu'il fallait faire en cas d'accident majeur. La Cour a statué que les graves atteintes à l'environnement pouvaient toucher le bien-être des personnes et les priver de la jouissance de leur domicile, portant ainsi atteinte à leur vie privée et familiale. En conséquence, les autorités italiennes avaient une obligation positive de fournir aux requérantes les informations nécessaires pour évaluer les risques pouvant résulter du fait de vivre dans une ville à proximité d'une usine chimique à haut risque. La non-fourniture aux requérantes de ces informations essentielles était une atteinte aux droits qui étaient les leurs en vertu de l'article 8[191]. La décision était particulièrement importante étant donné qu'il apparaît que l'État n'avait pas les informations demandées et qu'il lui faudrait donc les obtenir.

Dans l'affaire *McGinley et Egan*, les requérants avaient été exposés à des radiations lors d'essais nucléaires dans les îles Christmas et avaient demandé d'accéder aux dossiers concernant les risques potentiels pour la santé de cette exposition. La Cour a statué que les requérants avaient effectivement le droit d'accéder aux

---

189 Leander, note 183, par. 48, 67.
190 Gaskin, note 184, par. 49.
191 Guerra, note 185, par. 60.

informations en question en vertu des articles 6 et 8 de la Convention européenne des droits de l'homme, relatifs respectivement au droit d'être entendu équitablement et au droit au respect de la vie privée. Toutefois, le gouvernement avait rempli ses obligations positives en établissant un processus permettant d'obtenir l'accès aux informations, processus que les requérants n'avaient pas utilisé[192].

Dans l'affaire Odièvre, la question était celle de l'accès à des informations sur la mère biologique de la requérante. La Cour a admis l'existence d'une ingérence dans le droit au respect de la vie privée, tel que garanti par l'article 8, mais elle a statué que le refus des autorités françaises de fournir les informations représentait un équilibre approprié entre les intérêts de la requérante et ceux de sa mère, qui avait expressément souhaité que son identité soit tenue secrète[193].

Dans l'affaire Roche, qui comme McGinley et Egan invoquait des problèmes médicaux résultant d'essais militaires, la Cour a statué qu'il y avait eu une atteinte au droit au respect de la vie privée étant donné que le gouvernement n'avait pas de motifs raisonnables de refuser de divulguer les informations. Il faut noter que la Cour a estimé que les diverses divulgations effectuées en réponse aux demandes ne constituaient pas « le mode structuré de divulgation qu'envisage l'article 8 de la Convention »[194].

Quatrièmement, au moins dans certaines affaires, notamment Rotaru c. Roumanie, la Cour s'est référée au droit de réfuter des informations apparemment fausses[195]. L'affaire concernait des informations détenues par les services de sécurité qui étaient apparemment fausses, et auxquelles le requérant s'était vu refuser l'accès et la possibilité de les rectifier.

Il ressort clairement de ces décisions que la collecte et la divulgation d'informations privées, y compris dans le secteur public, soulèvent presque toujours des questions de pertinence par rapport à la vie privée. De plus, lorsqu'elle détermine si cette collecte et cette divulgation sont nécessaires dans une société démocratique, la Cour évalue l'utilisation donnée aux informations. La Cour s'est aussi référée au droit de réfuter (et peut-être par voie de conséquence de rectifier) les informations lorsque la personne concernée les juge inexactes. La Cour a au moins reconnu l'importance des organes de contrôle indépendants, et peut même exiger leur existence pour trancher les problèmes de protection des données.

Toutefois, lorsqu'il s'agit d'accès aux informations, et même aux informations personnelles relatives au requérant, la Cour a procédé avec précaution. Elle a refusé de reconnaître un droit général d'accès des individus à leurs informations personnelles, limitant la portée de ses décisions au cas par cas. Dans chaque affaire, elle a d'abord entrepris de déterminer si l'accès aux informations était ou non nécessaire pour protéger le droit du requérant au respect de sa vie privée et/ou familiale. Autrement dit, l'accès a été accordé lorsqu'il le fallait pour protéger un autre intérêt au respect de la vie privée, mais l'accès lui-même n'a pas été reconnu lui-même comme un intérêt au respect de la vie privée. De plus,

192 McGinley et Egan, note 186, par. 102-103.
193 Odièvre, note 187, par. 44-49.
194 Roche, note 188, par. 166.
195 Note 158, par. 46.

dans chacune de ces affaires, les informations étaient détenues par un organisme public. Il est loin d'être clair que la Cour appliquerait le même raisonnement, au moyen d'une obligation positive imposée à l'État, pour exiger la divulgation des informations par des organes privés.

La Cour européenne des droits de l'homme a été saisie de quelques affaires basées directement sur la vie privée et l'Internet. Ces affaires donnent à penser que le caractère complexe et assez différent de l'Internet peut soulever quelques questions épineuses concernant la vie privée. Ainsi, dans l'affaire K.U. c. Finlande, la question était celle de savoir si un FAI devait être contraint à révéler l'identité d'une personne qui avait utilisé ses services pour afficher une annonce se présentant comme provenant de quelqu'un d'autre, à savoir un garçon de 12 ans, contenant un « lien » vers une photographie du garçon et indiquant qu'il recherchait une « relation intime » avec un garçon de son âge ou plus âgé afin qu'il lui « montre comment on fait »[196]. Le FAI a refusé et ce refus a été admis par les tribunaux internes étant donné qu'en vertu de la loi finlandaise la police ne pouvait imposer la divulgation de ces informations que dans certains types d'affaires, ce qui n'incluait pas le cas décrit plus haut, qui était un cas de diffamation.

Pour se prononcer, la Cour a passé en revue un large éventail de documents internationaux du Conseil de l'Europe, de l'Organisation des Nations Unies et de l'Union européenne. Elle n'a pas eu de difficulté à estimer que l'affaire concernait la vie privée, « notion qui recouvre l'intégrité physique et morale de la personne »[197]. La Cour a noté que les États ont une obligation positive, en vertu de l'article 8, de sanctionner pénalement les infractions contre les personnes, particulièrement quand elles impliquent des enfants et autres personnes vulnérables, mais ces sanctions n'avaient qu'un effet dissuasif limité s'il était impossible d'identifier l'auteur de l'infraction. La possibilité de réclamer des dommages-intérêts au FAI n'était pas non plus suffisante, étant donné que seule une voie d'action directe contre l'auteur effectif de l'infraction pouvait créer l'effet dissuasif nécessaire.

La Cour a noté la nécessité de protections adéquates de la présomption d'innocence et le fait que « la liberté d'expression et la confidentialité sont des préoccupations primordiales et les utilisateurs des télécommunications et des services Internet doivent avoir une garantie que leur intimité et leur liberté d'expression seront respectées ». Toutefois, en se contentant d'exclure la divulgation des informations, l'État n'avait pas mis en place « un cadre permettant de concilier les différents intérêts à protéger dans ce contexte » et violait ainsi ses obligations au titre de l'article 8[198]. La Cour a donc reconnu la complexité de l'équilibre des droits à ménager pour trancher ce cas, mais elle n'a pas entrepris de mener elle-même cet exercice d'équilibrage.

3.1.2 Protection des données

3.1.2.1 Normes mondiales

Les régimes de protection des données intéressent directement la protection de la vie privée sur l'Internet, étant donné qu'ils ont été spécifiquement conçus pour traiter les questions de collecte des données et de confidentialité du type de celles qu'ont amenées

---

196 2 décembre 2008, Requête n° 2872/02, par. 7.
197 Ibid., par. 41.
198 Ibid., par. 46-50.

les technologies modernes. À un niveau très général, ces régimes subordonnent à certaines conditions la collecte, l'utilisation et le stockage des données personnelles (règles régissant les responsables du traitement de données), confèrent certains droits aux individus auxquels se rapportent les données (sujets des données) et mettent en place un système de supervision pour garantir le respect des règles et traiter les violations. Un aspect central de presque tous les systèmes de protection des données est l'identification de principes clés gouvernant ces questions et, en particulier, la collecte, l'utilisation et le stockage des données personnelles.

À l'Organisation des Nations Unies, la résolution 45/195, Principes directeurs pour la réglementation des fichiers personnels informatisés[199], énonce dix principes clés sur la protection des données. Ces principes s'appliquent principalement à la législation nationale, mais ils sont aussi contraignants pour les organisations intergouvernementales, sous réserve des modifications appropriées. Ils s'appliquent aussi aux fichiers informatisés détenus par des organes publics et privés contenant des données sur les personnes, et ils peuvent être étendus aux fichiers manuels et/ou aux données relatives à des personnes morales.

Les Principes directeurs incluent un certain nombre de principes gouvernant la collecte et l'utilisation des données personnelles que l'on retrouve dans quantité de régimes de protection des données. Les principes clés peuvent se résumer comme suit :

Licéité et loyauté : la collecte des données doit être loyale et licite et ne pas être contraire aux buts et aux principes de la Charte des Nations Unies.

Exactitude : les responsables du traitement de données sont tenus de vérifier régulièrement l'exactitude et la pertinence des données et de veiller à ce qu'elles demeurent aussi complètes que possible pour éviter les erreurs par omission.

Finalité : la finalité en vue de laquelle les données sont collectées doit être légitime et portée à l'attention de la personne concernée, les données ne doivent pas être utilisées à d'autres fins incompatibles, et elles ne doivent être conservées qu'aussi longtemps qu'elles sont nécessaires pour atteindre leur finalité première.

Accès par les personnes concernées : les sujets des données ont le droit de savoir quand les données les concernant sont collectées ou traitées, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs et d'obtenir les rectifications ou suppressions adéquates.

Non-discrimination : les dérogations à ces principes ne peuvent pas être de nature discriminatoire.

Sécurité : des mesures appropriées doivent être prises pour protéger les données contre les risques tant naturels qu'humains, tels que l'accès non autorisé, l'utilisation détournée ou la contamination physique.

Les Principes directeurs reconnaissent qu'il peut être nécessaire de déroger aux cinq premiers principes, mais seulement pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publique, ainsi que les droits et libertés d'autrui. Ils demandent que soit désignée une autorité de supervision indépendante chargée de contrôler le

---

199 Adoptée le 14 décembre 1990, A/RES/45/95.

respect des principes, et que soient mis en place des systèmes de sanctions en cas de violation des règles. Ils demandent aussi des limitations de la circulation des informations destinées aux pays n'offrant pas de garanties comparables.

XIV) Normes régionales sur la protection des données

Il y a de nombreuses normes régionales sur la protection des données. Les principaux systèmes existants sont les suivants :

- Organisation de coopération et de développement économiques (OCDE) : *les Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* de 1980[200].
- Forum de la coopération économique Asie-Pacifique (APEC) : *l'APEC Privacy Framework* de 2005.
- Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) : Acte additionnel A/SA.1/01.10 relatif à la protection des données à caractère personnel au sein de la CEDEAO[201].
- Organisation des États américains (OEA) : Résolution 2661 de l'Assemblée générale sur l'accès à l'information publique et la protection des données personnelles[202].
- Conseil de l'Europe : *Convention de 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel*[203], telle qu'amendée par le Protocole additionnel de 2001 à la Convention pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données[204].
- Union européenne : Directive 95/46/CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[205].

200 Adoptées par le Conseil de l'OCDE le 23 septembre 1980.
201 Adopté le 16 février 2010.
202 Adoptée le 7 juillet 2004, AG/RES.2661 (XLI-O/11).
203 Adoptée le 28 janvier 1981, STE n° 108, entrée en vigueur le 1er octobre 1985.
204 Adopté le 8 novembre 2001, STE n° 181, entré en vigueur le 1er juillet 2004.
205 Adoptée le 24 octobre 2001, JO L 281, telle que complétée par la Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant la protection des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201, p. 37, et par la Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/EC, JO L, p. 54.

3.1.2.2 Normes de l'APEC

La coopération économique Asie-Pacifique (APEC) compte 21 membres ; elle rassemble des pays tels que le Canada, le Chili, le Pérou et les États-Unis d'Amérique d'un côté du Pacifique et un certain nombre de pays d'Asie, dont de grandes économies telles que la Chine, le Japon et la Fédération de Russie, ainsi que l'Indonésie, le Viet Nam et la Thaïlande et des pays comme l'Australie et la Nouvelle-Zélande.

Les principales règles de l'APEC en matière de protection de la vie privée sont énoncées dans l'APEC Privacy Framework[206] (Cadre de l'APEC relatif à la protection de la vie privée). Le préambule du Cadre base clairement la motivation de son adoption sur la nécessité de conserver la confiance des consommateurs de manière à promouvoir les avantages économiques du commerce électronique. Il note que le Cadre est conforme aux Lignes directrices de l'OCDE, et qu'il ménage un équilibre entre les besoins de confidentialité des informations et les besoins du commerce. Il reconnaît aussi la nécessité de permettre aux différents pays une certaine flexibilité dans la mise en œuvre du Cadre.

Les principes de base sont en gros similaires par nature aux Principes directeurs de l'ONU, ainsi qu'aux normes européennes et aux normes de l'OCDE. Un certain degré de flexibilité est intégré dans le cadre, ce qui peut contraster avec les normes européennes, plus détaillées, où les exceptions sont davantage précisées. Cela se reflète aussi dans les dispositions sur l'application, qui laissent aux économies membres une grande latitude pour décider de la meilleure approche.

Les principes du Cadre définissent de façon large les informations personnelles comme toutes les informations sur une personne identifiée ou identifiable, de même qu'un responsable du traitement des informations personnelles est défini comme une personne qui exerce un contrôle sur la collecte ou l'utilisation des informations personnelles (paragraphes 9-10). Comme il a déjà été noté, le Cadre intègre spécifiquement un élément de flexibilité dans son application, sur la base des différences sociales, économiques et culturelles, ainsi que la nécessité de protéger la sécurité nationale, la sûreté publique et la politique publique (paragraphes 12-13).

Le premier principe de fond est d'empêcher de nuire, ce qui appelle des mesures visant à prévenir les utilisations abusives des informations personnelles, mesures proportionnées à la probabilité et à la gravité des risques (paragraphe 14). Les responsables du traitement sont tenus d'aviser, si possible à l'avance ou au moment de la collecte, les personnes sur le fait de collecter des informations personnelles, les fins auxquelles elles sont collectées et comment contacter le responsable du traitement (paragraphes 15-17). Seules les informations utiles aux fins indiquées doivent être collectées, et elles doivent l'être par des moyens licites et loyaux (paragraphe 18).

Les informations ne doivent être utilisées qu'aux fins pour lesquelles elles ont été collectées, ou à des fins compatibles, sauf avec le consentement de la personne concernée ou si nécessaire pour fournir un service demandé par la personne (paragraphe 19). Les personnes doivent aussi se voir offrir un choix quant à la collecte, l'utilisation et la divulgation de leurs informations (paragraphe 20). Les informations doivent être exactes

---

206 Disponible à l'adresse http://publications.apec.org/publication-detail.php?pub_id=390.

et tenues à jour, et stockées de façon à réduire au minimum le risque d'accès non autorisé, de modification, etc. (paragraphes 21-22).

Conformément aux principes de base de la protection des données, les personnes doivent avoir le droit d'accéder aux informations les concernant et de les rectifier, sous réserve du coût et de diverses autres contraintes (paragraphes 23-25). Enfin, les responsables du traitement doivent être tenus pour responsables de l'application de ces principes, y compris en garantissant que ceux auxquels les informations sont transférées s'engagent à respecter les principes (paragraphe 26).

3.1.2.3 Normes européennes

Il existe des différences notables entre les divers régimes régionaux de protection des données, bien que le système de l'Union européenne soit très proche de celui du Conseil de l'Europe, tel qu'amendé. Nous donnons ici une description plus détaillée du système de l'Union européenne, à titre d'exemple d'une approche forte de la protection des données et aussi d'un système qui a exercé une grande influence dans le monde.

Le système mis en place par l'Union européenne est largement reconnu à la fois comme très progressiste en ce sens qu'il offre une forte protection aux données et comme jouant un rôle de leadership dans ce domaine, en ce sens qu'il influe sur les lois de protection des données dans d'autres pays. Les règles sont juridiquement contraignantes pour les 27 membres de l'Union européenne, mais leur influence s'étend beaucoup plus loin. Dans une récente étude, Greenleaf compare les systèmes européens aux systèmes de l'OCDE et de l'APEC et identifie dix différences essentielles entre eux, qui reflètent toutes le niveau plus élevé des normes dans les systèmes européens. Analysant 29 lois extra-européennes de protection des données, il conclut que 13 incorporent au moins neuf de ces dix caractéristiques, 19 en comportent au moins sept et 23 au moins cinq, soit la moitié[207]. Cette très forte corrélation donne à penser que les systèmes européens sont assez dominants au niveau mondial.

L'Union européenne a adopté en décembre 2000 une Charte des droits fondamentaux de l'Union européenne[208] qui prévoit une forte protection à la fois de la vie privée en général (article 7) et des données en particulier (article 8). Ce dernier article dispose que les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement. Les personnes ont le droit d'accéder aux données les concernant et d'en obtenir la rectification, et le respect de ces règles est soumis au contrôle d'une autorité indépendante. Bien que cette disposition ait été adoptée après les dispositions principales du cadre de protection des données, ces dernières doivent être considérées à la lumière de ces garanties primordiales.

L'approche fondamentale de la Directive 95/46 consiste à appliquer les règles de façon extrêmement large et ensuite appliquer les limitations ou exceptions. Les définitions de l'article 2 définissent ainsi les données à caractère personnel comme toute information concernant une personne physique identifiée ou identifiable, le traitement des données comme toute opération appliquée à des données à caractère personnel (dont la collecte,

---

207 Voir par exemple Greenleaf, G. The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, University of New South Wales Faculty of Law Research Series, Paper 42, 2011.

208 2000/C 364/01.

le stockage, etc.), et responsable du traitement comme la personne physique ou morale qui détermine les finalités et les moyens du traitement des données.

Conformément à ces définitions, toute personne qui stocke des numéros de téléphone sur un téléphone mobile ou un ordinateur est un responsable du traitement. Cependant, l'article 3 dispose que la Directive ne s'applique pas au traitement de données à des fins qui ne relèvent pas du champ d'application du droit communautaire (comprenant la sécurité et les activités relatives au droit pénal) ni au traitement effectué par une personne physique pour l'exercice d'activités « exclusivement personnelles ou domestiques ». Il limite aussi le champ d'application de la Directive au traitement automatisé en tout ou en partie (c'est-à-dire essentiellement électronique) ou aux données figurant dans un fichier, excluant ainsi les données stockées ad hoc ou d'une façon informelle.

Les principes de la protection des données sont énoncés à l'article 6 (voir encadré). Ce sont pour l'essentiel les mêmes que les trois premiers principes énumérés dans la résolution 45/95 de la résolution de l'Assemblée générale des Nations Unies. La plupart des principes sont raisonnablement clairs. En gros, la règle relative aux traitements incompatibles n'est pas enfreinte si les informations sont utilisées « comme ceux qui les ont fournies pourraient s'attendre à ce qu'elles soient utilisées et divulguées »[209].

XV) Principes de la Directive sur la protection des données

La Directive 95/46 de l'UE énonce les principes de base de la protection des données à l'article 6. Ces principes requièrent que les données à caractère personnel soient :

(a) traitées loyalement et licitement ;

(b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ;

(c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

(d) exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

(e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

---

209 Commissaire irlandais à la protection des données, Règle 3 sur la protection des données : utilisation et traitement ultérieur des informations personnelles. Disponible à l'adresse http://dataprotection.ie/viewdoc.asp?DocID=25.

L'article 7 de la Directive 95/46 énonce les conditions auxquelles est subordonné le traitement des données, qui comprennent le consentement de la personne concernée, le fait qu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, la nécessité du traitement pour respecter une obligation légale du responsable du traitement, la nécessité du traitement pour sauvegarder « l'intérêt vital » de la personne concernée (comme la collecte de sang après un accident), la nécessité du traitement pour l'exécution publique d'une mission d'intérêt public ou relevant de l'exercice d'une autorité publique, ou la nécessité du traitement pour la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées. Dans ces deux derniers cas, la personne concernée peut s'opposer au traitement pour des « raisons prépondérantes et légitimes », et un droit d'opposition distinct est prévu en ce qui concerne le traitement des données à des fins de prospection (article 14). Il est évident que cette liste est à la fois intrinsèquement large et sujette à des interprétations larges et potentiellement divergentes.

Le consentement de la personne concernée est un élément clé du système et il faut qu'il soit dépourvu d'ambiguïté. Cependant, le fait de cocher la case d'acceptation des termes et conditions, comme on le fait souvent pour les services Internet, satisfait à ce critère. C'est le cas même si le plus souvent les personnes concernées ne lisent pas ces termes et conditions, et auraient peut-être du mal à les comprendre si elles les lisaient. Cette pratique pourrait être critiquée parce qu'elle fait peser une charge indue sur les personnes concernées, mais toute l'idée de contrôle sur ses données personnelles conduit presque inévitablement à ce résultat.

Les articles 10 à 12 de la Directive définissent certains droits de la personne concernée. Aux termes des articles 10 et 11, la personne concernée doit être informée de l'identité du responsable du traitement ou de son représentant, des finalités du traitement et de toutes informations supplémentaires, telles que les destinataires des données et le droit d'accès et de rectification des données, nécessaires pour assurer un traitement loyal des données. La rigueur de cette disposition est en partie atténuée par la règle selon laquelle les informations en question n'ont pas besoin d'être fournies à la personne concernée si celle-ci a déjà été informée. De plus, dans le cas d'un traitement effectué par une entité qui n'a pas collecté les données, ces informations n'ont pas besoin d'être fournies si le traitement a une finalité de recherche historique ou scientifique, lorsque l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si le traitement est exigé par la loi.

Aux termes de l'article 12, toute personne concernée a le droit d'obtenir du responsable du traitement, à des intervalles raisonnables et sans délais ou frais excessifs :

- la confirmation que les données la concernant sont traitées, les finalités du traitement, les catégories de données visées et les destinataires des données ;
- la communication des données sous une forme intelligible, ainsi que leur origine ;
- la logique qui sous-tend tout traitement automatisé des données, au moins dans le cas où cela peut conduire à une décision la concernant.

Les responsables du traitement sont aussi tenus de rectifier, d'effacer ou de verrouiller les données dont le traitement n'est pas conforme à la directive, notamment parce que les données sont inexactes ou incomplètes, et d'en informer les tiers. Les articles 16 et 17 disposent que les données doivent être conservées et traitées en en assurant la sécurité.

L'article 13 autorise les États à limiter la portée des obligations visées aux articles 6, 10, 11, 12 et 21 (voir ci-dessous) si nécessaire pour protéger la sécurité nationale ou publique, prévenir les infractions pénales ou professionnelles, pour des raisons économiques importantes, à des fins de contrôle ou de réglementation, ou pour protéger la personne concernée ou les droits ou libertés d'autrui.

Une autre règle apparemment sévère, mais là encore atténuée par des exceptions, est l'obligation imposée aux responsables du traitement de notifier à l'autorité de contrôle (avant le traitement des données) les finalités des traitements, les catégories de personnes concernées, les destinataires et les éventuels transferts de données à destination de pays tiers. Un registre des traitements notifiés de cette manière doit être tenu par l'autorité de contrôle ; ce registre peut être consulté par toute personne[210]. Les États peuvent prévoir de larges exceptions à cette règle, y compris au bénéfice d'organisations à but non lucratif, lorsque les responsables du traitement désignent des détachés à la protection des données, dans le cas de registres destinés, en vertu de la loi, à l'information du public et pour certaines catégories de traitements qui ne risquent pas de nuire aux droits ou libertés. Pour les traitements qui sont couverts par une exception, les informations clés doivent être mises à la disposition de toute personne sur demande (articles 18, 19 et 21).

XVI) Vue d'ensemble du système de protection des données de l'Union européenne

Les principaux éléments du système sont les suivants :

- Larges définitions des données personnelles et du traitement des données
- Principes gouvernant les données personnelles : les données sont traitées loyalement, à des fins spécifiques identifiées, les traitements doivent être adéquats, pertinents et non excessifs à ces fins, et les données doivent être exactes et à jour, et conservées pas plus longtemps que nécessaire
- Droits de la personne concernée : être informée par le responsable du traitement de la finalité du traitement, obtenir les données sous une forme intelligible, exiger la rectification ou l'effacement des données
- Obligation du responsable du traitement de notification à l'autorité de contrôle aux fins de la tenue d'un registre public
- Voies de recours à la disposition des personnes concernées
- Transferts de données uniquement là où une protection adéquate est assurée
- Supervision par une autorité indépendante

210 Un exemple est celui du registre des responsables du traitement de données au Royaume-Uni, disponible en format consultable à l'adresse http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx.

Diverses voies de recours sont disponibles, dont le droit des personnes concernées d'obtenir du responsable du traitement réparation du préjudice subi du fait d'un traitement illicite des données (article 23) et recours juridictionnel en cas de violation des droits des personnes concernées (article 22). Des sanctions sont aussi prévues à l'encontre des auteurs de violations des règles (article 24).

Un élément clé de la Directive est constitué par les restrictions qu'elle impose aux transferts de données faisant l'objet d'un traitement vers des pays tiers (c'est-à-dire extérieurs à l'Union européenne) (article 25). Un tel transfert ne peut avoir lieu que si le pays tiers assure aux données un « niveau de protection adéquat ». Là encore, des exceptions sont admises, et les États peuvent prévoir de transférer des données à des pays n'assurant pas un niveau de protection adéquat pour des motifs qui sont dans une large mesure les mêmes que ceux qui sont invoqués pour les traitements légitimes, à l'exception du premier motif (à savoir l'intérêt poursuivi par le responsable du traitement ou un tiers) (article 26).

Des pays entiers peuvent être certifiés par la Commission comme assurant un niveau de protection adéquat. Cela a été fait pour des pays comme la Suisse, le Canada et l'Argentine[211]. Aux États-Unis d'Amérique, qui ne sont généralement pas considérés comme assurant un niveau de protection adéquat en raison de l'absence de législation centrale gouvernant la protection des données des acteurs privés, le Ministère du commerce a élaboré un International Safe Harbor Privacy Principles Certification Program[212]. Il s'agit d'un programme fondé sur le volontariat, en vertu duquel les sociétés peuvent demander leur certification lorsqu'elles se conforment aux sept Safe Harbor Principles. Ceux-ci sont alignés sur les règles européennes de protection des données et incluent la notification sur les finalités de la collecte des données, le droit des personnes de refuser à l'avenir le transfert des données à des tiers ou leur utilisation à d'autres fins, les impératifs de sécurité pour les données, etc.[213]. Une fois certifiées, les sociétés en question sont considérées comme assurant un niveau adéquat de protection des données personnelles au regard des règles de l'UE[214].

La Directive prévoit deux types de structures institutionnelles. Tout d'abord, chaque partie doit établir une autorité de contrôle indépendante investie de divers pouvoirs – d'investigation, d'intervention, y compris d'interdiction d'un traitement, d'ester en justice et de se saisir de demandes (article 28). En second lieu, il y a le Groupe de protection dit de l'article 29, composé de représentants des autorités de contrôle, dont le rôle est essentiellement consultatif (articles 29 et 30).

Il ne fait guère de doute que la Directive joue un rôle très important dans la protection des données personnelles. Elle est largement louée pour sa neutralité technologique (à savoir qu'elle s'applique quelle que soit la technologie utilisée pour traiter les données), pour son imposition de normes élevées qui sont fondées sur des principes flexibles et pour l'harmonisation qu'elle instaure entre les règles au sein de l'Union européenne et dans une certaine mesure plus largement.

---

211 Voir http://ec.europa.eu/justice/policies/privacy/thirdcountries/index_en.htm.

212 Voir http://export.gov/safeharbor.

213 On peut trouver une liste complète des principes à l'adresse http://export.gov/safeharbor/eu/eg_main_018475.asp.

214 Le système a été approuvé par la Commission européenne dans sa décision 2000/520/CE. Voir http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

Cependant, on lui a reproché d'être dépassée (ce qui est compréhensible étant donné la rapidité du changement en termes de traitement des données personnelles), trop bureaucratique, rigide et prescriptive, insuffisamment ciblée sur les risques au lieu des procédures, et même irréaliste (par exemple en ce qui concerne les transferts internationaux dans le contexte de flux mondiaux de données massifs et croissants)[215].

La nécessité de revoir la Directive est largement admise et des consultations sont en cours dans cette perspective. La Commission européenne décrit les objectifs de cet exercice comme étant de moderniser le système pour relever les défis de la mondialisation et des nouvelles technologies, de renforcer les droits tout en réduisant les formalités administratives, d'assurer la libre circulation des données, d'améliorer la clarté et la cohérence des règles, et de réaliser une mise en œuvre cohérente et efficace[216].

Le 25 janvier 2012, la Commission a publié ses propositions « finales » concernant un règlement (et non plus une directive) sur la protection des données[217]. Le point majeur de cette transformation est que le règlement aurait force de loi dans chaque État membre[218]. La proposition comprend un certain nombre de dispositions visant à renforcer les règles de la Directive, à clarifier les zones d'incertitude et certaines définitions, et à « muscler » divers systèmes, tels que les informations à fournir aux personnes concernées, les procédures de mise en œuvre des droits de ces personnes, les voies de recours, les pouvoirs de contrôle et la coopération.

Le projet de règlement propose aussi un certain nombre de nouvelles règles. Les informations à fournir aux personnes concernées doivent être transparentes, facilement accessibles et compréhensibles. Une autre règle est le droit à la portabilité des données, y compris le droit d'obtenir une copie de ses données dans un format couramment utilisé. Les responsables du traitement sont tenus de mettre en place des politiques et des mécanismes internes pour garantir le respect de leurs obligations, de notifier aux personnes concernées les violations des données et de mener des évaluations avant les traitements à risque. Les organismes publics et les grands organismes privés sont tenus de désigner des délégués à la protection des données. Il est aussi proposé de créer un nouvel organe, le Comité européen de la protection des données, pour remplacer le Groupe de protection de l'article 29, avec des pouvoirs élargis. Les règles relatives à l'établissement du « niveau de protection adéquat » aux fins des transferts à des pays tiers sont aussi clarifiées.

Certaines des propositions prêtent peut-être plus à controverse. Par exemple, le nouveau règlement propose de s'appliquer aux opérations de traitement des données basées

215 Voir par exemple Robinson, N. ; Graux, H. ; Botterman, M. et Valieri, L. Review of EU Data Protection Directive: Summary, prepared for the UK Information Commissioner's Office, May 2009, Foreword. Disponible à l'adresse http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf.

216 Voir http://ec.europa.eu/justice/policies/privacy/review/index_en.htm.

217 Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données), Bruxelles, 25.1.2012, COM(2012) 11 final, 2012/0011(COD).

218 Les directives, pour leur part, ne font qu'obliger les États membres à adapter leur législation pour qu'elle respecte leurs dispositions.

en dehors de l'Union européenne, « lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées, ou à l'observation de leur comportement ». Il créerait un « droit à l'oubli », comprenant un droit d'obtenir que les données soient effacées et ne soient plus traitées.

3.1.2.4 Règles additionnelles

La Directive 95/46 est complétée par deux autres directives, la Directive 2002/58 concernant la protection des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques) et la Directive 2006/24 sur la conservation des données[219]. La première prévoit un certain nombre de règles particulières concernant la protection de la vie privée dans le contexte des communications électroniques, exigeant la confidentialité des communications et de divers autres types de données (données relatives au trafic et données de localisation), sauf à des fins limitées – telles que la facturation, la commercialisation et les services à valeur ajoutée – et prévoyant des droits des usagers en ce qui concerne diverses questions en rapport avec la communication – telles que la facturation détaillée, les services d'identification des appels, le renvoi automatique des appels, les annuaires d'abonnés et les communications non sollicitées. Les États peuvent, par des mesures législatives, déroger aux règles relatives à la confidentialité à des fins de sécurité nationale et publique et d'enquête sur les infractions pénales – qui toutes sont extérieures aux domaines de compétence de l'Union européenne – y compris en prévoyant la conservation des données.

La Directive sur la conservation des données fait fi, pour l'essentiel, de ces règles en exigeant la conservation générale d'un grand nombre de catégories de données de communication – sans inclure le contenu des communications – durant une période de six mois à deux ans, en dérogation aux dispositions pertinentes sur la non-conservation figurant dans la Directive vie privée et communications électroniques.

XVII) Décisions constitutionnelles sur la Directive de l'UE sur la conservation des données[220]

Les tribunaux de trois pays – la République tchèque, l'Allemagne et la Roumanie – ont déclaré inconstitutionnelles, pour des motifs de protection de la vie privée, les règles nationales transposant la Directive de l'UE sur la conservation des données. En octobre 2009, la Cour constitutionnelle roumaine a statué que la Directive était contraire à l'article 8 de la Convention européenne des droits de l'homme. La Cour a noté entre autres le caractère global de l'exigence de conservation des données, qui s'applique à toutes les personnes, qu'elles aient commis ou même soient soupçonnées d'avoir commis un crime ou un délit. Elle a noté que le champ

---

219 Note 205.

220 Les informations de cette section sont tirées du rapport d'évaluation parallèle d'EDRI sur la Directive concernant la conservation des données (2006/24/CE), 17 avril 2011, disponible à l'adresse http://www.edri.org/files/shadow_drd_report_110417.pdf, et du Rapport de la Commission au Parlement européen : rapport d'évaluation concernant la Directive sur la conservation des données (Directive 2006/24/CE), Bruxelles, le 18.4.2011 COM(2011) 225 final.

d'application de la Directive était flou et que les règles ne comportaient pas de protections suffisantes contre les abus[221]. Cette décision est particulièrement importante dans la mesure où elle affirme être fondée sur l'article 8 de la Convention européenne des droits de l'homme. Si la Cour européenne des droits de l'homme devait faire sienne cette interprétation, cela voudrait dire que les pays de l'Union européenne seraient enfermés dans une impasse juridique.

En mars 2010, la Cour constitutionnelle fédérale allemande a suivi cet exemple, affirmant que les règles de transposition allemandes violaient le droit constitutionnel au secret des télécommunications. Elle a noté que les règles créeraient chez les citoyens le sentiment d'être surveillés, ce qui compromettrait leur jouissance de divers droits fondamentaux. Une conservation limitée des données, destinée à sauvegarder d'importants intérêts tenant à la sécurité, pouvait être justifiée, les règles en question avaient une portée trop large. La Cour a aussi mentionné l'absence de sauvegardes et, en particulier, le défaut de contrôle approprié[222].

La Cour constitutionnelle tchèque a de même statué, en mars 2011, qu'étant donné l'intensité et l'ampleur de l'ingérence dans la vie privée, les règles ne pouvaient se justifier comme une limitation nécessaire du droit au respect de la vie privée. Elle a noté à cet égard qu'une conservation du type de celle qui était requise par les règles n'avait pas d'impact notable sur les statistiques de la criminalité, surtout au vu des nouvelles possibilités technologiques d'éviter l'identification. Comme la Cour allemande, la Cour tchèque a noté que les finalités qui justifieraient la conservation étaient trop larges et que les sauvegardes prévues étaient insuffisantes[223].

Selon la Commission européenne, « Des affaires relatives à la conservation des données ont également été portées devant la Cour constitutionnelle bulgare, ce qui a entraîné une révision de la loi de transposition, devant la Cour constitutionnelle chypriote, qui a jugé inconstitutionnelles les ordonnances des tribunaux rendues en vertu de la loi de transposition, et devant la Cour constitutionnelle hongroise, où une affaire concernant l'absence de mention, dans la loi de transposition, des finalités juridiques du traitement des données, est pendante[224] [225].

---

221 Décision n° 1258 du 8 octobre 2009 de la Cour constitutionnelle roumaine, journal officiel roumain n° 789 du 23 novembre 2009. Disponible à l'adresse http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

222 Jugement du Bundesverfassungsgericht 1 BvR 256/08, du 2 mars 2010. Disponible à l'adresse http://www.bverfg.de/en/press/bvg10- 011en.html.

223 Journal officiel du 1er avril 2011, jugement de la Cour constitutionnelle du 22 mars sur les dispositions de l'article 97, paragraphes 3 et 4, de la Loi n° 127/2005 Coll. sur les communications électroniques et la modification de certaines lois telles qu'amendées, et Décret n° 485/2005 sur la conservation des données et leur transmission aux autorités compétentes. Disponible à l'adresse http://www.concourt.cz/clanek/GetFile? id=5075.

224 Cour administrative suprême de Bulgarie, arrêt n° 13627 du 11 décembre 2008 ; Cour suprême de Chypre, affaires n° 65/2009, 78/2009, 82/2009 et 15/2010-22/2010, 1er février 2011 ; le recours constitutionnel en Hongrie a été introduit par l'Union hongroise pour les libertés civiles le 2 juin 2008.

225 Rapport de la Commission au Parlement européen : rapport d'évaluation concernant la Directive sur la conservation des données (Directive 2006/24/CE), note 220, p. 24.

La Directive a été massivement critiquée, par la société civile comme par des organes officiels de la Commission. Par exemple, le Contrôleur européen de la protection des données a décrit la Directive comme « l'instrument le plus préjudiciable au respect de la vie privée jamais adopté par l'UE »[226]. European Digital Rights (EDRI) a déclaré : « Durant les cinq dernières années, la Directive sur la conservation des données s'est avérée une violation inutile et sans précédent des droits fondamentaux de 500 millions d'Européens »[227]. Les tribunaux de trois pays – Croatie, Allemagne et Roumanie – ont déclaré inconstitutionnelles les lois de transposition de la Directive, et elle est attaquée pour inconstitutionnalité dans d'autres pays également (voir encadré). EDRI a recommandé à sa place « un système de préservation accélérée et de collecte ciblée des données relatives au trafic pour faciliter une enquête spécifique (« préservation des données »), comme convenu au niveau international dans la Convention sur la cybercriminalité adoptée par le Conseil de l'Europe en 2001 »[228].

Le Rapport de la Commission au Parlement européen : rapport d'évaluation concernant la Directive sur la conservation des données (Directive 2006/24/CE), évaluation officielle de la Directive par la Commission, n'est pas d'accord. Il dit : « L'évaluation a montré que la conservation des données est très utile aux systèmes de justice pénale et aux services répressifs de l'UE » et « L'UE devrait continuer, grâce à des règles communes, à veiller à ce que des normes élevées soient constamment imposées au stockage, à l'extraction et à l'utilisation des données relatives au trafic et des données de localisation »[229]. En conséquence, il propose de réviser plutôt que d'abroger le cadre actuel de la conservation des données.

En 2009, une nouvelle directive a été adoptée, qui modifie et étend certaines dispositions de la Directive vie privée et communications électroniques[230]. La Directive de 2009 a renforcé les règles sur la sécurité et les notifications aux usagers en cas de violation de la sécurité. Cependant, le changement le plus important a consisté en quelques mots de l'article 5(3), qui dit maintenant que le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un utilisateur n'est permis qu'à condition que l'utilisateur ait donné son accord. Il suffisait précédemment de fournir aux utilisateurs des informations claires et détaillées sur le stockage et l'accès dans l'équipement terminal et de leur offrir la possibilité d'exclure ces activités.

---

226 Voir son discours du 3 décembre 2010. Disponible à l'adresse http://www.edps.europa.eu/EDPSWeb/Webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_FR.pdf.

227 Rapport d'évaluation parallèle sur la Directive concernant la conservation des données (2006/24/CE), note 220, p. 2.

228 Ibid., p. 6.

229 Note 220, p. 1.

230 Directive 2009/136/CE du Parlement européen et du Conseil modifiant la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO L337, p. 11.

La Directive est appelée familièrement « directive cookies » en raison de l'énorme impact qu'aura l'application de cette règle sur le fonctionnement des cookies. Elle a causé une forte réaction de l'industrie, qui estime qu'il sera difficile, coûteux et peu pratique de la mettre en œuvre[231]. La règle a aussi suscité nombre de questions sur ce qui exactement constitue un consentement. Par exemple, le paramétrage d'un navigateur pour qu'il accepte les cookies, ce qui était fondamentalement la pratique dans le passé, vaut-il consentement ? Sans doute pas, mais exiger des utilisateurs qu'ils donnent leur accord à toute tentative de placer un cookie sur leurs appareils serait aussi impraticable.

La Directive reste en vigueur et les pays prennent des mesures pour la mettre en œuvre (la date limite était mai 2011 ; voir ci-dessous à propos des efforts de la France). Au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, une loi a été adoptée – du reste, le Royaume-Uni a été un des premiers pays à adopter une telle loi – mais le Bureau du Commissaire à l'information, qui est chargé de la mise en œuvre, a indiqué qu'il laissera un an aux sociétés pour s'y conformer (c'est-à-dire qu'il ne poursuivra pas en justice les contrevenants durant un an)[232]. L'impact réel de la mesure reste donc largement à déterminer.

3.2 Protection de la vie privée au niveau national

3.2.1 Chine

La protection accordée à la vie privée est limitée en Chine, en l'absence de véritable garantie constitutionnelle, de loi appropriée sur le respect de la vie privée et de loi sur la protection des données. En règle générale, les autorités chinoises exercent un contrôle considérable sur l'Internet et les individus ont très peu de moyens pour préserver leur vie privée contre ces autorités[233].

Cependant, des pressions croissantes s'exercent en faveur du changement, surtout en ce qui concerne les menaces contre le respect de la vie privée venant de sources privées. Ces pressions ont principalement pour origine les utilisations abusives de données privées sous la forme d'approches de marketing ciblées suite à des transactions commerciales comme l'achat d'une voiture ou d'assurances ou l'ouverture d'un compte bancaire. Ces approches prennent souvent la forme hautement intrusive de SMS ciblés ou même d'appels téléphoniques de suivi.

En conséquence, un certain nombre de propositions juridiques et réglementaires ont été formulées ou adoptées ces dernières années. Des modifications des lois pénales et des lois sur la responsabilité civile ont institué des actions en justice indépendantes en faveur du respect de la vie privée, et diverses propositions ont été faites en ce qui concerne la protection des données.

---

231 Voir http://online.wsj.com/article/SB10001424052748704444304575628610624607130.html.

232 Voir http://econsultancy.com/us/blog/8210-q-a-lbi-s-manley-on-preparing-for-the-eu-cookie-laws.

233 Voir par exemple les informations fournies à ce sujet par Reporters sans frontières, à l'adresse http://fr.rsf.org/chine.html, les bulletins d'information de la FIJ sur la campagne pour la liberté de la presse en Chine à l'adresse http://asiapacific.ifj.org/en/pages/asia-pacific-china-bulletin-2008, et le chapitre sur la Chine, et en particulier la surveillance, dans Privacy and Human Rights 2006, note 119, p. 335.

Contrairement à beaucoup de constitutions, la Constitution chinoise ne prévoit pas de droit général et indépendant au respect de la vie privée. L'article 40 de la Constitution est libellé comme suit :

La liberté et la confidentialité de la correspondance des citoyens de la République populaire de Chine sont protégées par la loi. Aucune organisation ou personne ne peut, pour quelque motif que ce soit, leur porter atteinte, sauf dans les cas où, pour répondre aux besoins de la sûreté de l'État ou des enquêtes pénales, les organes de la sécurité publique ou les parquets sont autorisés à censurer la correspondance conformément aux procédures prescrites par la loi[234].

Cette disposition établit un droit sectoriel limité au respect de la vie privée en ce qui concerne la correspondance, mais ce droit est assorti de larges exceptions, qui ne sont limitées que par la condition selon laquelle elles doivent être établies par la loi. L'article 38 de la Constitution prévoit une protection générale de la dignité personnelle des citoyens, en disposant que « les insultes, la diffamation et les accusations mensongères sont interdites ». Cette disposition a été interprétée par les tribunaux comme offrant une base générale au droit au respect de la vie privée, en tant que lié à la notion plus large de réputation. La protection de la réputation, que l'on trouve à l'article 101 des Principes généraux du droit civil (1986)[235], a aussi servi de base à la protection de la vie privée. Toutefois, cela ne joue que lorsqu'il y a eu aussi une atteinte préalable à la réputation, si bien que la portée de la protection de la vie privée proprement dite est assez limitée.

Le Septième Amendement à la Loi pénale a introduit certaines dispositions pénales en rapport avec le respect de la vie privée. Les employés d'organismes publics, ou d'organisations financières, des télécommunications, des transports, de l'éducation ou de la santé ont l'interdiction de vendre ou de diffuser par un autre moyen illicite les informations personnelles qu'ils ont obtenues dans l'exercice de leurs fonctions. Les auteurs d'infractions à cette règle sont condamnés à une peine d'emprisonnement d'au moins trois ans si le comportement visé atteint un certain niveau de gravité. Quiconque obtient de telles informations par un vol ou un autre moyen illicite est passible de la même peine, là encore si le comportement visé atteint un certain niveau de gravité. Les organisations qui commettent ces infractions sont passibles de pénalités financières, et leurs directeurs et autres responsables sont passibles des mêmes peines que les personnes physiques qui commettent de telles infractions[236].

Cet amendement est important en ce qu'il représente la première action indépendante concernant les atteintes à la vie privée en Chine. Cependant, comme beaucoup de lois nationales chinoises, il se situe à un niveau très général et ne définit pas des termes clés tels que « informations personnelles », autres moyens illicites de diffusion, et le niveau de gravité à atteindre pour que la responsabilité soit engagée. La première condamnation en application de ces dispositions aurait été prononcée le 3 janvier 2010 par un tribunal de Zhuhai, au sujet de l'achat et de la revente subséquente d'un journal d'appels téléphoniques provenant d'un haut fonctionnaire.

---

234 Disponible à l'adresse http://www.npc.gov.cn/englishnpc/Constitution/node_2825.htm.

235 Adoptés le 12 avril 1986. Disponibles à l'adresse http://en.chinacourt.org/public/detail.php?id=2696.

236 McKenzie et Milner, China Update, mars 2009: Recent Developments in Data Protection, 9 mars 2009 (Morrison Foerster). Disponible à l'adresse http://www.mofo.com/international/CN_en/news/15332.html.

Un autre fait nouveau important a été l'adoption le 26 décembre 2009 de la Loi sur la responsabilité civile, qui est entrée en vigueur le 1er juillet 2010. Cette loi a institué un quasi-délit distinct relatif à la vie privée, donnant naissance à un droit privé d'action en dommages-intérêts. La partie qui affirme qu'il a été porté atteinte à son droit au respect de la vie privée, peut revendiquer tous les profits obtenus par la partie adverse, ainsi que des dommages-intérêts pour préjudice moral. Un opérateur de site Web qui apprend ou est informé que le droit au respect de la vie privée ou d'autres droits d'une autre partie ont été violés en raison de contenus hébergés sur son site et ne supprime pas ces contenus est solidairement responsable avec la personne qui a affiché les contenus. De plus, si la partie plaignante demande les coordonnées de la partie qui a affiché les contenus, l'opérateur du site Web doit soit fournir cette information, ou sinon devenir directement responsable de ces contenus. Ces règles posent problème du point de vue de la liberté d'expression parce que (entre autres) elles n'exigent pas de preuve que les matériels portent effectivement atteinte au droit au respect de la vie privée avant de pouvoir être supprimés. Enfin, les établissements de santé peuvent être poursuivis au civil s'ils sont responsables de divulgations non autorisées des dossiers médicaux des patients[237].

Cela représente une importante extension des protections pénales préexistantes. Particulièrement pertinent est le fait que ces dispositions confèrent aux individus un droit d'agir eux-mêmes en justice pour protéger leurs droits au respect de la vie privée.

Il y a eu des propositions visant à introduire une véritable loi de protection des données en Chine, mais elles n'ont pas encore abouti. En 2006-2007, une loi de protection des données personnelles, rédigée par l'Institut de droit de l'Académie des sciences chinoise, a été examinée par le Comité d'informatique du Conseil d'État, mais ce comité n'existe plus. Greenleaf décrit comme suit la situation :

En Chine, les lois sur la confidentialité des données sont depuis cinq ans dans ce qu'on peut appeler la période des « Royaumes guerriers », les royaumes en question étant les nombreux fiefs des bureaucraties labyrinthiques de la RPC[238].

XVIII) République de Corée : règle des noms réels

En juillet 2007, la République de Corée a adopté la Loi sur la vérification des noms réels. Dans sa version actuelle, cette loi impose à tous les sites Web comptant au moins 100 000 visiteurs par jour l'obligation d'identifier les usagers qui transfèrent des matériels ou affichent des commentaires par leur nom réel, c'est-à-dire en pratique au moyen des numéros d'enregistrement des résidents (RRN). La loi vise à résoudre des problèmes tels que le nombre croissant d'accusations diffamatoires

237 Voir Hunton & Williams, Client Alert, janvier 2010. Disponible à l'adresse http://www.hunton.com/files/News/4bfa5361-4d8f-4c7e-af03-75055a82202c/Presentation/NewsAttachment/7d2612ba-40d6-4884-83de-c01965341d41/new_chinese_tort_liability_law.pdf. Voir aussi McKenzie, P. et Milner, G. Data Privacy in China: Criminal Law Developments, 25 janiver 2010 (Morrison Foerster). Disponible à l'adresse http://www.mofo.com/data-privacy-in-china-civil-and-criminal-law-developments-01-25-2010/.

238 Greenleaf, G., "Asia-Pacific data privacy: 2011, year of revolution?" [2011] UNSWLRS 30, p. 5. Disponible à l'adresse http://law.bepress.com/unswwps/flrps11/art30/.

et frauduleuses portées en ligne, les immixtions dans la vie privée et le harcèlement en ligne.

Techniquement, les règles n'exigent pas des sociétés qu'elles créent des bases de données des informations personnelles étant donné qu'elles peuvent obliger les usagers à fournir les données chaque fois qu'ils se connectent. Cependant, cela n'est pas praticable vu que la plupart des usagers ne seraient pas disposés à procéder ainsi. Google a refusé de se conformer à la loi et a préféré empêcher les usagers de transférer des contenus sur la version coréenne de YouTube, pour le motif que les règles de vérification des noms réels « ne cadrent pas avec les principes de Google »[239].

Une violation massive des données survenue en juillet 2011, dans laquelle les hackers auraient volé les données personnelles de 35 millions de Coréens à la société SK Communications (voir encadré supra), a conduit à renouveler les appels en faveur de l'abrogation de la loi, qui a aggravé les effets de la fuite. Fin décembre 2011, l'autorité coréenne de régulation de l'Internet, la Commission des communications de Corée, a indiqué qu'elle réexaminerait la politique suivie et le consensus semble être que la loi va probablement être abrogée[240].

Un autre fait nouveau important a été la publication en février 2011 du projet de Principes directeurs de la technologie de la sécurité de l'information pour la protection des informations personnelles. Les Principes directeurs ont été élaborés conjointement par le Ministère de l'industrie et de la technologie de l'information, l'Administration chinoise de la normalisation, et l'Administration générale du contrôle de la qualité, de l'inspection et de la quarantaine ; ils constituent un ensemble de règles non contraignantes concernant la protection des données.

Les Principes directeurs, qui s'appliquent aux informations traitées sur les ordinateurs, donnent une définition large des informations personnelles, à savoir toute information qui, seule ou combinée avec d'autres, peut servir à identifier une personne. Le but du traitement (y compris la collecte) des informations personnelles doit être clair et raisonnable, et les personnes concernées doivent être informées du but et de l'entité qui traite les données, ainsi que de leurs droits (qui comprennent ceux d'accéder aux données, de les rectifier et de s'opposer à la poursuite de leur traitement) et des moyens de se plaindre. Seules les données qui sont appropriées au but déclaré peuvent être collectées. Les données doivent être tenues confidentielles et elles ne doivent être utilisées que dans le but déclaré, à moins qu'un autre but ne soit prévu par la loi ou clairement agréé par la personne concernée. Des règles spéciales sont applicables à certains types de données particulièrement sensibles. Le consentement d'un tuteur est requis avant que les données provenant de personnes âgées de moins de 16 ans puissent être traitées.

239 Voir Reuters, South Korea's net nirvana spawns good, bad and ugly results, 5 décembre 2011. Disponible à l'adresse http://www.msnbc.msn.com/id/45562846/ns/technology_and_science-tech_and_gadgets/t/south-koreas-net-nirvana-spawns-good-bad-ugly-results/#.Tw6t7Jj6QTM. Voir aussi http://www.zdnet.com/blog/foremski/google-refuses-compliance-with-korean-real-name-law-but-imposes-it-on-g-users/1920.

240 Voir http://www.hancinema.net/real-name-internet-law-on-way-out-36915.html.

Les Principes directeurs comportent des règles strictes concernant le transfert des données. Le transfert à des tiers n'est permis qu'avec le consentement de la personne concernée, lorsqu'il est prévu par la loi ou lorsque l'autorité de contrôle l'autorise. Contrairement à ce qui est le cas dans d'autres systèmes, il n'est pas prévu d'exceptions, ce qui fait que ce système est très contraignant et peut-être même impraticable.

Les règles relatives aux transferts à l'étranger sont encore plus rigides, étant donné que pareil transfert n'est permis que s'il est autorisé par la loi ou approuvé par l'autorité de contrôle (et même pas lorsque la personne concernée donne son consentement). Étant donné qu'il n'y a pas actuellement de loi qui autorise ces transferts (ce qui est peut-être compréhensible vu que la question ne s'est pas posée auparavant), et qu'il n'y a pas d'exceptions à l'exigence d'une autorisation spécifique (de la loi ou de l'autorité de contrôle), ces règles représentent un obstacle très difficile à franchir pour les flux transfrontières de données.

Comme les Principes directeurs ne sont pas contraignants, ils peuvent dans une certaine mesure être testés aisément dans la pratique, peut-être en prélude à l'adoption de normes juridiquement contraignantes. C'est tout aussi bien, car dans leur forme actuelle, ils sont jugés impraticables par certains[241].

Un certain nombre de dispositions des lois et des principes directeurs chinois adoptés depuis 2009 offrent une protection sectorielle aux données personnelles dans les domaines du blanchiment de fonds, des dossiers médicaux, des assurances, de la protection des consommateurs et des évaluations de solvabilité[242]. Il y a aussi eu quelques activités législatives/réglementaires au niveau local (provinces et municipalités) afin de protéger la vie privée, par exemple dans les lois sur la consommation et en relation avec les systèmes informatiques[243].

3.2.2 Inde

Jusqu'à une époque récente, l'Asie du Sud était très en retard pour ce qui est de protéger les données et plus généralement la vie privée, conduisant un auteur à la décrire en 2009 comme la « dernière frontière » de la protection des données en Asie[244]. Quelques années plus tard, la situation avait notablement changé, au moins en Inde.

La Constitution indienne ne prévoit pas de droit indépendant au respect de la vie privée, mais la Cour suprême a identifié un tel droit essentiellement dans l'article 21, relatif au droit à la vie et à la liberté, qui se lit comme suit : « Nul ne peut être privé de la vie ou de la liberté personnelle si ce n'est conformément à une procédure établie par la loi ». Ainsi, dans un jugement de 1994, la Cour suprême a statué :

---

241 McKenzie, P. ; Dicker, A. et Fang, J. China Issues New Guidelines on Data Privacy Protection, 11 avril 2011 (Morrison Foerster), disponible à l'adresse http://www.mofo.com/files/Uploads/Images/110411-China-Data-Privacy-Guidelines.pdf; Fernández, China Publishes Draft Privacy Guidelines, 14 avril 2011 (Hogan Lovells), disponible à l'adresse http://www.hldataprotection.com/2011/04/articles/international-eu-privacy/china-publishes-draft-privacy-guidelines/; Ross, L., Gao, K., et Zhou, A., China Issues Draft Guidelines on Online Privacy, Announces new Agency to Supervise the Internet, 19 mai 2011 (Wilmer Hale).

242 Voir Greenleaf, note 207, p. 7.

243 Voir McKenzie et Milner, note 236.

244 Greenleaf, G., "Twenty-one years of Asia-Pacific data protection" (2009) 100 Privacy Laws & Business International Newsletter 21.

> Le droit au respect de la vie privée est implicite dans le droit à la vie et à la liberté garanti aux citoyens de ce pays par l'article 21. C'est le « droit d'être laissé en paix ». Un citoyen a le droit de préserver son intimité – famille, mariage, procréation, maternité et éducation, entre autres aspects. Nul ne peut publier quoi que ce soit sur les aspects susmentionnés sans son consentement. Quiconque le ferait violerait le droit au respect de la vie privée de la personne concernée et serait considéré comme responsable si une action en réparation était engagée[245].

Il n'y a toujours pas de loi civile indépendante sur le respect de la vie privée en Inde, bien qu'une telle loi soit en discussion depuis plusieurs années. Cependant, suite au jugement de 1994 susmentionné, les tribunaux ont dû trouver un moyen de réparation contre les immixtions dans la vie privée, étant donné que la Cour suprême avait déclaré dans ce jugement que la publication de faits privés, « exacts ou non », serait une atteinte au droit au respect de la vie privée. À cet effet, les tribunaux se sont appuyés essentiellement sur les règles générales de la common law telles que l'abus de confiance.

Un projet de loi détaillé sur le respect de la vie privée est en discussion en Inde depuis quelque temps, mais il n'a toujours pas été adopté. Un projet daté du 19 avril 2011, intitulé « Third Working Draft (for Discussion and Correction) Legislative Department » a été initialement divulgué suite à une fuite mais est maintenant disponible en ligne[246]. Ce texte créerait un large droit indépendant au respect de la vie privée, ainsi qu'un mécanisme robuste pour répondre aux violations du droit, appelé l'Autorité indienne de protection des données (DPAI).

Le projet de loi donne une définition large de la vie privée, incluant des éléments tels que la confidentialité des communications, la vie privée et familiale, les informations bancaires et médicales, la protection des données et diverses protections contre les actions de l'État, par exemple dans les domaines de la perquisition et de la surveillance. Il faut noter que la loi ne serait applicable qu'aux citoyens indiens, ce qui exclut de son champ d'application les très importantes activités indiennes d'externalisation. Certains régimes juridiques préexistants, dont ceux qui concernent le droit à l'information et la corruption, sont spécifiquement exemptés de l'application de la loi, mais il semble que le projet de loi préserverait toutes les lois préexistantes en la matière (voir l'article 3).

La DPAI disposerait de larges pouvoirs, dont ceux d'enregistrer les responsables du traitement de données, d'enquêter sur les abus et d'obliger les responsables du traitement de données à prendre certaines mesures pour mettre fin aux abus. La DPAI aurait aussi le pouvoir de se saisir de certaines plaintes (pas encore spécifiées). Les plaignants pourraient aussi s'adresser au Cyber Regulations Appellate Tribunal, établi en application de l'article 48 de la Loi sur la technologie de l'information (Information Technology Act) de 2000[247], qui aurait le pouvoir, entre autres, d'imposer une indemnisation pour les

---

245 R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632. Ce jugement a étendu le droit au respect de la vie privée en imposant à l'État l'obligation d'empêcher les immixtions dans la vie privée. Le droit a été reconnu initialement par la Cour suprême dans l'affaire Govind v. State of Madhya Pradesh & Anr (1975), SCR (3) 946.

246 Disponible à l'adresse http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf.

247 n° 21 de 2000.

violations de la loi[248]. Cependant, comme on l'a noté, le texte reste un projet de loi qui pourrait subir des modifications importantes avant d'être adopté.

Diverses lois indiennes assurent une protection contre les immixtions de l'État dans la vie privée, par exemple dans le domaine de l'action répressive, bien que comme dans tous les pays elles soient sujettes à des dérogations. Ainsi, le Code pénal exige que la police obtienne des mandats avant de conduire une perquisition. Ces règles sont modifiées par la jurisprudence constitutionnelle de la Cour suprême qui a par exemple statué que les écoutes téléphoniques sont une grave ingérence dans la vie privée qui, en conséquence, nécessite un niveau élevé de justification[249].

Les télécommunications sont généralement protégées en application de l'Indian Telegraph Act de 1885[250] ainsi que de l'Information Technology Act de 2000. Cette dernière loi, telle qu'amendée, a institué une infraction pénale limitée pour certaines violations de la vie privée en ligne[251]. Les amendements apportés à cette dernière loi en 2008 ont prévu l'interception des télécommunications lorsqu'il est nécessaire ou approprié de protéger la souveraineté, l'intégrité ou la sécurité de l'Inde, les relations amicales avec les autres États, l'ordre public, ou de lutter contre l'incitation au crime ou les entraves aux enquêtes sur les infractions[252]. L'Autorité indienne de régulation des télécommunications (TRAI), créée par le Telecommunications Regulatory Authority of India Act de 1997[253], est aussi investie de larges pouvoirs dans ce domaine, et elle a émis diverses injonctions juridiques pour protéger la confidentialité des communications[254].

Il faut aussi mentionner ici la Loi sur le droit à l'information (Right to Information Act) de 2005[255], qui garantit l'accès à toutes les informations détenues par les autorités publiques, à l'exclusion de toute autre loi interdisant cet accès, sous réserve des seules exceptions qu'elle prévoit. L'article 8(j) de la Loi protège la vie privée en ces termes :

Les informations relatives aux informations personnelles dont la divulgation est sans rapport avec aucune activité publique ou aucun intérêt public, ou qui serait la cause d'une ingérence injustifiée dans la vie privée de la personne, à moins que le Central Public Information Officier (responsable de l'information du public au niveau national), le State Public Information Officier (responsable de l'information du public au niveau des États) ou l'autorité d'appel, selon le cas, n'estime que l'intérêt général justifie la divulgation de ces informations :

---

248 Pour en savoir plus sur le projet de loi sur le respect de la vie privée, voir Gupta, A., “Analysis of the Privacy Bill, 2011” on India Law and Technology Blog, 27 juin 2011 et Greenleaf, G., “India's U-turns on Data Privacy” série de quatre articles publiés dans (2011) 110-114 Privacy Laws & Business International Report.

249 Voir People's Union for Civil Liberties (PUCL) v. Union of India and Anr. (1997) 1 SCC 301.

250 n° 13 de 1885. Voir par exemple les articles 5 et 7.

251 Voir l'article 66-E.

252 Information Technology (Amendment) Act, 2008, No. 10 de 2009, article 34, modifiant l'article 69 de la loi initiale et introduisant les nouveaux articles 69A et 69B.

253 n° 24 de 1997.

254 Voir par exemple les directives de l'article 13, à lire en conjonction avec le sous-alinéa (i) de l'alinéa (b) du paragraphe (1) de l'article 11 du Telecom Regulatory Authority of India Act, 1997 (n° 24 de 1997), visant à garantir le respect par les fournisseurs d'accès des termes et conditions de la licence concernant la confidentialité des informations sur les abonnés et la confidentialité des communications, 26 février 2010.

255 n° 22 de 2005.

Étant entendu que les informations qui ne peuvent être refusées au Parlement ou à l'organe législatif d'un État ne sont refusées à aucune personne.

Cette disposition exige un intérêt public prépondérant pour supprimer la confidentialité.

Enfin et surtout, le 11 avril 2011, le Ministère indien des communications et de la technologie de l'information a adopté les Règles sur la technologie de l'information (pratiques et procédures raisonnables en matière de sécurité et données ou informations personnelles sensibles) de 2011. C'est essentiellement un mini-régime de protection des données qui ressemble beaucoup aux régimes mis en place dans d'autres pays. Une particularité intéressante est que ces règles s'appliquent exclusivement au secteur privé, alors que dans la plupart des autres pays les règles similaires s'appliquent d'abord et avant tout au secteur public et ensuite éventuellement au secteur privé.

Quant au fond, les règles obligent les responsables du traitement de données à mettre en place des politiques de protection des données qui décrivent clairement leurs pratiques et leur politique, indiquent le type de données collectées, les finalités de cette collecte, la divulgation des informations et les mesures de sécurité en place pour les protéger (article 4). Le champ d'application de beaucoup de ces règles se limite aux données personnelles sensibles, telles que les informations médicales ou financières, mais les données incluent aussi les informations sur l'orientation sexuelle. Les règles requièrent aussi une notification raisonnable concernant la collecte et les finalités de la collecte des données personnelles, ainsi que les destinataires concernés. Les données ne peuvent être utilisées qu'aux fins indiquées et il y a aussi des règles relatives à l'accès aux données et à leur rectification, ainsi qu'à la sécurité (article 5). La conformité avec la norme IS/ISO/IEC 27001 « Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information » est censée assurer une sécurité suffisante des informations (article 8).

Bien que le champ d'application exact de ces règles reste à déterminer, et qu'elles restent limitées par rapport aux règles adoptées dans de nombreux pays, il est vrai aussi de dire que l'adoption de ces règles a porté l'Inde à un niveau inédit de protection des données personnelles.

3.2.3 Égypte

Historiquement, la protection de la vie privée n'a pas été une priorité en Égypte. Les forces de sécurité pouvaient accéder à quantité d'informations personnelles, en ligne ou hors ligne, même si officiellement la question était réglementée par le Code de procédure pénale. Il n'y a pas de loi consacrée à la protection de la vie privée. Il reste à déterminer si cela va changer avec la révolution et les grands changements démocratiques qu'elle a apportés.

À l'heure de la rédaction de la présente publication, la Constitution égyptienne était la Déclaration constitutionnelle proclamée par le Conseil suprême des forces armées le 23 mars 2011, à la suite d'un référendum organisé le 19 mars 2011 concernant neuf articles transitoires. La Déclaration contient, outre ces neuf articles, 49 articles repris de la Constitution de 1971, dont l'article 11 (dans la nouvelle numérotation), qui se lit comme suit :

> L'inviolabilité de la vie privée des citoyens est protégée par la loi. La correspondance, les appels téléphoniques et autres moyens privés et confidentiels de communication ne peuvent être confisqués, soumis à enquête ou surveillés que sur la base d'un mandat judiciaire et pour une question spécifique, conformément aux dispositions de la loi.

À l'heure de la rédaction de la présente publication, il n'y avait pas de loi d'ensemble sur la protection de la vie privée, ni de loi sur la protection des données. On trouve des règles relatives à la vie privée dans un certain nombre d'éléments de la législation sectorielle mais elles sont souvent contradictoires. Un bon exemple est celui des règles relatives à la protection de la vie privée dans la loi sur les télécommunications[256]. L'article 13, qui décrit le rôle de l'Autorité nationale de régulation des télécommunications, dispose que l'Autorité suit la mise en œuvre des licences de télécommunications afin de s'assurer que les droits des usagers, et « en particulier le droit au respect de leur vie privée » sont respectés.

Toutefois, l'article 64 dispose que tous les fournisseurs de services de télécommunications doivent veiller à ce que leurs systèmes disposent du potentiel technique voulu pour « permettre aux forces armées et aux entités de la sécurité nationale d'exercer leurs pouvoirs dans le cadre de la loi ». Officiellement, cela doit être fait « en tenant dûment compte de l'inviolabilité des citoyens, protégée par la loi » mais le caractère général de l'article 64, ainsi que le ciblage global du cadre juridique, a fait que cette sauvegarde a été dans une large mesure ignorée en pratique dans le passé.

L'article 58 de la loi oblige l'Autorité à tenir une base de données des titulaires des licences les autorisant à utiliser le spectre des fréquences, précisant que cette « base de données doit être classifiée afin de protéger la vie privée » des titulaires de licences. Dans la plupart des pays, ces informations sont rendues publiques, sur la base du principe que le spectre des fréquences est une ressource publique et que le public a le droit de savoir qui a obtenu une licence pour l'utiliser.

3.2.4 France

La France est un pays qui est fier de la forte protection dont y jouit la vie privée. Bien que cette position bénéficie généralement d'un fort soutien de la nation, le système a été de plus en plus mis en question à la suite de l'affaire Strauss-Kahn, dans laquelle il a été considéré que la protection indue accordée à la vie privée des riches et des célébrités empêchait les médias de faire la lumière sur les actes historiquement immoraux prêtés à Strauss-Kahn[257].

Il est donc surprenant que la Constitution française de 1958 ne prévoie pas de protection explicite de la vie privée. Toutefois, en 1995, le Conseil constitutionnel a statué que le

---

256 Loi sur la régulation des télécommunications, n° 10 de 2003.

257 Voir par exemple Gopnik, A., D.S.K.: French Lives, French Laws, 16 mai 2001. Disponible à l'adresse http://www.newyorker.com/online/blogs/newsdesk/2011/05/dsk-french-lives-french-law.html.

droit était implicitement contenu dans la Constitution[258], et il a confirmé cette position dans une décision de 1999[259].

L'article 9 du Code civil, ajouté en 1970[260], assure la protection de la vie privée, disant simplement : « Chacun a droit au respect de sa vie privée ». Le deuxième alinéa de cet article indique clairement que les tribunaux peuvent, outre la réparation du préjudice, prescrire toutes mesures, telles que « séquestre, saisie et autres, propres à empêcher ou faire cesser » une atteinte à l'intimité de la vie privée, et ce en référé s'il y a urgence. Ces règles sont appliquées via l'article 1382 du Code civil qui établit les principes généraux de la responsabilité civile.

Dans la pratique, les tribunaux français appliquent ces règles généreusement, interprétant la vie privée comme englobant entre autres la vie amoureuse, les amitiés, les vicissitudes familiales, les activités de loisir, les opinions politiques, les affiliations syndicales et religieuses, et l'état de santé[261].

La France a aussi adopté des dispositions pénales sévères sur le respect de la vie privée, que l'on trouve aux articles 226-1 à 7 du Code pénal. Aux termes de l'article 226-1, est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait de porter volontairement atteinte à l'intimité de la vie privée d'autrui :

(1) en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

(2) en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Le consentement est néanmoins présumé lorsque ces actes ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire. Ces dispositions, qui ne concernent que les lieux privés et les propos confidentiels, sont largement considérées comme visant principalement les paparazzis.

L'article 226-2, qui vise plutôt les médias, punit des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide d'un des actes prévus par l'article 226-1. L'article 42 de la Loi sur la liberté de la presse du 29 juillet 1881, attribue normalement la responsabilité de ces délits, lorsqu'ils sont commis par la voie de la presse, au directeur de la publication. Aux termes de l'article 226-6, dans les cas prévus par ces articles, l'action publique ne peut être exercée que sur plainte de la victime.

---

258 Décision n° 94-352 DC du 18 janvier 1995, Recueil, p. 170 - Journal officiel du 21 janvier 1995, p. 1154. Disponible à l'adresse http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html.

259 Décision n° 99-416 DC du 23 juillet 1999, Recueil, p. 100 - Journal officiel du 28 juillet 1999, p. 1125. Disponible à l'adresse http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-416-dc/decision-n-99-416-dc-du-23-juillet-1999.11847.html. Voir en particulier le par. 45.

260 Loi n° 70-643 du 17 juillet 1970.

261 Voir ambafrance-us.org/spip.php?article640.

La Loi n° 91-646 du 10 juillet 1991, relative au secret des correspondances émises par la voie des communications électroniques, protège, comme son titre l'indique, le secret des communications électroniques. Aux termes de son article 3, l'interception des communications peut à titre exceptionnel être autorisée à des fins telles que le maintien de la sécurité, la lutte contre le terrorisme ou la criminalité, ou pour protéger des intérêts économiques ou scientifiques essentiels du pays. Des procédures strictes gouvernent l'autorisation de ces interceptions, en vertu de l'article 4 (il faut qu'elles soient autorisées au final par le Premier Ministre ou par une ou deux personnes spécialement déléguées par lui).

La France est aussi dotée depuis longtemps d'un régime robuste de protection des données personnelles, sous la forme de la Loi sur la protection des données de 1978[262]. Telle qu'amendée, cette loi applique intégralement la Directive de l'UE sur la protection des données, notamment en établissant la Commission nationale de l'informatique et des libertés (CNIL) en tant qu'autorité de contrôle indépendante. Une caractéristique intéressante de la loi française est qu'elle oblige les responsables du traitement de données à définir une durée de conservation compatible avec la finalité envisagée (article 30(1)(5)).

La France a aussi appliqué la Directive de l'UE sur la conservation des données, qui oblige les fournisseurs de services de télécommunications à conserver les données relatives au trafic pendant une durée d'un an. Cette mise en application est contestée devant le Conseil d'État, qui est la plus haute juridiction administrative française, par une vingtaine de sociétés de l'Internet exerçant des activités en France[263].

La France a entrepris d'appliquer la Directive 2009/136 de l'UE, appelée la « directive cookies ». Une ordonnance donnant effet à la Directive a été adoptée par le Conseil des ministres le 24 août 2011. Les usagers devront désormais être informés sur l'installation et l'utilisation des cookies, ce qui selon les règles doit être fait avant l'installation du premier cookie. Toutefois, selon la règle française, si les navigateurs sont paramétrés pour permettre aux programmes d'installer des cookies, la situation par défaut sur la plupart des ordinateurs est que les usagers ne sont pas obligés de donner leur consentement explicite[264]. Cela semble être une solution plus susceptible de satisfaire les intérêts de l'industrie que de tracer la voie vers une forte protection de la confidentialité, et il reste à déterminer si elle sera acceptable en tant que moyen d'appliquer la Directive.

---

262 Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, telle qu'amendée par la Loi n° 2004-801 du 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel.

263 Voir News Wires, Internet giants challenge French data law over privacy, 6 avril 2011. Disponible à l'adresse http://www.france24.com/en/20110406-internet-giants-challenge-france-data-law-privacy-google-facebook-ebay. Il est difficile de déterminer où en est la procédure dans cette affaire à l'heure actuelle.

264 Voir http://www.privacysecuritysource.com/2011/09/09/france-implements-the-cookies-directive-and-strengthens-its-privacy-laws/.

XIX) Garanties constitutionnelles de la protection des données en Amérique latine

Un trait relativement exceptionnel des pays latino-américains est la forte prévalence de garanties constitutionnelles explicites de la protection des données ou du droit plus limité d'habeas data. Dans la plupart des autres pays, les garanties du respect de la vie privée sont assez génériques par nature mais selon certaines estimations près des deux tiers des constitutions latino-américaines prévoient cette protection explicite. En voici quelques exemples :

Mexique : L'article 6 de la Constitution dispose : « Chacun a droit à la protection de ses données personnelles » ;

Brésil : Article 5(LXXII) de la Constitution : « Le droit d'habeas data est accordé :

(a) pour garantir au demandeur la connaissance d'informations le concernant, figurant dans les registres ou les banques de données des services gouvernementaux ou des entités publiques ;
(b) pour rectifier les données, si le demandeur ne préfère pas suivre la voie secrète, judiciaire ou administrative ;

Uruguay : Article 66(19) de la Constitution : « Les droits suivants des personnes sont reconnus et garantis : le droit à la protection des informations personnelles, y compris le droit d'accéder aux informations et données de cette nature et de prendre des décisions à leur sujet. La collecte, la mise en fichiers, le traitement et la distribution ou diffusion de ces données ou informations requièrent l'autorisation de leur titulaire ou une ordonnance d'un tribunal ».

3.2.5 Argentine

La Constitution argentine inclut un droit indépendant au respect de la vie privée, similaire à celui qu'on trouve dans de nombreuses constitutions, à l'article 19, qui se lit comme suit :

> Les actes privés des hommes qui ne portent en aucune manière atteinte à l'ordre public et à la moralité publique et ne portent pas préjudice à un tiers ne concernent que Dieu et sont soustraits au pouvoir des juges. Aucun habitant de la Nation n'est obligé de faire ce que ne commande pas la loi, ni empêché de faire ce qu'elle n'interdit pas[265].

De plus, comme beaucoup de constitutions latino-américaines, elle prévoit un droit d'habeas data, à l'article 43, dans les termes suivants :

> Toute personne peut engager cette action pour prendre connaissance des données la concernant et de leur but, contenues dans les registres publics ou les banques de données publiques, ou dans les bases de données privées destinées à fournir des informations ; au cas où les données sont inexactes ou manifestent une discrimination, cette action peut être

265 Voir aussi l'affaire Ponzetti de Balbín, note 128.

> engagée pour demander la suppression, la rectification, la confidentialité ou la mise à jour de ces données. Le secret des sources d'information des journalistes est inviolable.

Le Code civil prévoit aussi une protection de la vie privée à l'article 1071bis[266], qui assure une large protection de la vie privée, lorsqu'aucune infraction pénale n'est en jeu. En cas de violation de la vie privée, le tribunal ordonne la cessation de l'activité d'ingérence, si elle n'a pas déjà pris fin, et peut aussi ordonner le paiement de dommages-intérêts. Si cela est équitable, le tribunal peut aussi exiger la publication du jugement dans un périodique ou un journal. Cet article est fréquemment appliqué en Argentine pour protéger divers types d'intérêts à la protection de la vie privée.

Dans une série de décisions, les tribunaux argentins ont ordonné des mesures provisoires contre les moteurs de recherche de Google et Yahoo![267]. Dans toutes ces affaires, des données personnelles du plaignant (toujours une célébrité ou un personnage connu) telles que son nom ou une image, avaient été affichées sur des sites Web de tiers sans son consentement, généralement pour promouvoir la vente de contenus ou de services sexuels. Au lieu de poursuivre les personnes directement responsables, les plaignants ont agi en justice contre les moteurs de recherche, probablement dans l'espoir de supprimer plus systématiquement l'accès.

Dans de nombreux cas, des mesures provisoires ont été ordonnées contre les moteurs de recherche, au motif qu'ils avaient aggravé cette violation des droits des plaignants au respect de la vie privée. Ces mesures ont souvent été ordonnées pour rompre leurs liens non seulement avec les sites Web cités, mais aussi avec des sites Web similaires. Non seulement cela est extrêmement difficile voire techniquement impossible à faire, mais il s'agit aussi d'une violation du droit international[268].

Il reste à déterminer comment cela tournera, bien que certaines des premières décisions aient maintenant été infirmées. Ainsi, dans l'affaire Virginia da Cunha c. Yahoo de Argentina y Otro[269], jugée en juillet 2009, des dommages-intérêts d'un montant de 50 000ARS (environ 12 000 dollars E.-U.) ont été infligés à Google comme à Yahoo!, mais en août 2010 cette décision a été infirmée par un arrêt (deux juges contre un) de la Cour d'appel[270].

Le Code pénal argentin, tel qu'amendé par la Loi n° 26.388 relative aux violations des communications électroniques et autres normes[271], prévoit des sanctions pour diverses infractions relatives aux technologies de l'information. Cette loi a été rebaptisée dans le Titre V du Chapitre III du Code pénal « Violation des secrets et de la vie privée ».

---

266 Ajouté par l'article premier de la Loi n° 21.173, publiée au Journal officiel le 22 octobre 1975.

267 Une grande partie des informations sur ces affaires sont empruntées à Compa, E. et Bertoni, E., Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad (Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)). Disponible à l'adresse http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf.

268 Voir par exemple la Déclaration de 2011 sur l'Internet et la liberté d'expression des quatre mandats internationaux sur la liberté d'expression, disponible à l'adresse http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

269 Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y perjuicios (Juz. Nac. En lo Civil nø 75, Expte. Nø 99.620/06), 29 juillet 2009.

270 Voir http://www.nytimes.com/2010/08/20/technology/internet/20google.html.

271 Publiée au Journal officiel du 25 juin 2008.

L'article 153, qui a trait aux violations des communications électroniques, considère comme un délit le fait d'accéder et d'obtenir sans consentement toute communication électronique, lettre, annexe, fax ou télégramme. Commet aussi un délit toute personne non autorisée qui supprime ou détourne des communications électroniques ou les intercepte ou enregistre. L'accès non autorisé à des bases de données et des systèmes de technologie de l'information privés ou publics et la fourniture à des tiers d'informations en provenant sont aussi des délits.

L'Argentine a été un des premiers pays d'Amérique latine à adopter une loi de protection des données, sous la forme de la Loi de 2000 sur la protection des données personnelles[272]. La forte protection accordée par cette loi aux données personnelles est reflétée par le fait que l'Argentine est le seul pays d'Amérique latine qui ait été reconnu par la Commission européenne comme assurant un niveau de protection adéquat aux données personnelles[273]. Il est apparent que la loi s'inspire des normes européennes en matière de protection des données[274].

3.2.6 Mexique

La Constitution mexicaine prévoit une large protection de la vie privée à l'article 16 qui dit, entre autres :

> Nul ne peut subir d'ingérence dans sa personne, sa famille, son domicile, sa correspondance ou ses biens, sauf en vertu d'un mandat écrit d'une autorité compétente, justifiant et motivant la cause légale de la procédure.
>
> Dans tous les mandats de perquisition, que l'autorité judiciaire est seule à pouvoir exécuter et qui doivent être écrits, le lieu à inspecter doit être indiqué, de même que la ou les personnes à appréhender et les objets à rechercher. Il est pris soin de limiter la perquisition à la finalité poursuivie et la perquisition se conclut par un acte circonstancié en présence de deux témoins choisis par l'occupant du lieu ou, en son absence ou s'il refuse, par les autorités exécutant la perquisition.
>
> Les communications privées sont inviolables. La loi punit pénalement tout acte portant atteinte à leur liberté et confidentialité. Seule l'autorité judiciaire fédérale peut, sur la demande de l'autorité fédérale qui applique la loi ou du responsable du Ministère public de l'entité fédérale concernée, autoriser l'interception de toute communication privée. À cet effet, l'autorité compétente doit établir et justifier les motifs juridiques de sa demande. Elle doit en outre indiquer le type de l'interception, les personnes concernées et sa durée. L'autorité judiciaire fédérale ne peut donner cette autorisation lorsqu'il s'agit de questions électorales, fiscales, commerciales, de travail ou administratives, ou dans le cas de communications d'un accusé avec son défenseur.

---

272 Loi 25.326, promulguée le 30 octobre 2000.

273 Voir http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

274 Dans son étude, Greenleaf estime que la loi argentine possède neuf des dix attributs du système européen qui font défaut dans le système de l'OCDE. Note 207, p. 10.

> Les interceptions autorisées doivent se conformer aux exigences et aux limites prévues par la loi. Les interceptions qui ne s'y conforment pas sont privées de toute valeur probante.
>
> L'autorité administrative ne peut visiter les domiciles que pour s'assurer qu'ils respectent les règlements de santé et de police et pour exiger la présentation des livres et documents indispensables pour vérifier que les résidents observent les dispositions fiscales, en veillant à cet égard au respect des lois et des formalités prescrites pour les perquisitions.
>
> La correspondance postale est exempte de tout examen et sa violation est punie par la loi.

La Constitution assure donc une forte protection de la vie privée en général, contre les perquisitions et pour la confidentialité des communications.

Le Code civil fédéral prévoit la protection sur le plan civil du droit au respect de la vie privée. Il prévoit spécifiquement des réparations pour le préjudice moral subi par une personne du fait d'actes illégaux préjudiciables à ses « sentiments, affections, croyances, honneur, réputation, vie privée, configuration ou aspects physiques, ou à l'opinion d'autrui à son sujet ». Cette disposition a donné lieu à des décisions de justice[275].

Depuis 2002, il existe une protection pour les données personnelles détenues au moins par les autorités publiques fédérales, en vertu de la Loi fédérale sur la transparence et l'accès aux informations publiques gouvernementales[276], qui est la loi mexicaine sur le droit à l'information ou la liberté de l'information. Bien que ce soit une loi sur le droit à l'information, un de ses buts est de « garantir la protection des informations personnelles détenues par des personnes ou entités désignées par la Loi » (article 4(III)). Le chapitre IV de la loi établit un régime de protection des informations personnelles qui comprend des règles telles que l'obligation de n'utiliser les données qu'aux fins pour lesquelles elles ont été collectées, de garantir la sécurité des données, de mettre à disposition un document exposant la politique d'utilisation des données, de veiller à la mise à jour et à l'exactitude des données, de ne pas les divulguer à des tiers (sauf dans certaines circonstances), d'informer l'autorité de contrôle du fait que des données personnelles sont collectées, et de permettre à la personne concernée d'accéder à ses données personnelles et de les rectifier. Le contrôle est assuré par l'Institut fédéral pour l'accès à l'information (IFAI, maintenant Institut fédéral pour l'accès à l'information et la protection des données).

La portée de la loi sur le droit à l'information est essentiellement limitée aux organes publics fédéraux. Toutefois, une loi générale de protection des données, contraignante pour les organes privés, a été adoptée en 2010 sous la forme de la Loi fédérale sur la protection des données personnelles détenues par des parties privées. Selon Greenleaf, cette loi ne respecte que cinq des dix principes clés européens de protection des données, puisque les cinq principes suivants ne sont pas pris en compte :

---

275 Voir par exemple Solís v Radiomovil Dipsa SA de CV (affaire 642/99), cité dans Schmidt, L. et Arceo, A. "Image and publicity rights in Mexico" dans World Trademark Review, septembre/octobre 2008.

276 Disponible à l'adresse http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/laweng.pdf. Disponible en espagnol, telle qu'amendée, à l'adresse http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf.

- collecte des données limitée à ce qui est nécessaire aux fins déclarées ;
- obligation d'adresser une notification à l'organe de protection des données en cas de collecte de données ;
- obligation d'anonymiser ou de détruire les données passé un certain délai ;
- limites au traitement automatisé des données ;
- obligation de prévoir une faculté d'opt-out pour les utilisations des données à des fins de marketing direct[277].

Cependant, la loi met en place la plupart des principes clés de protection des données que l'on trouve dans les autres systèmes[278]. La fonction de contrôle est là encore assurée par l'IFAI.

3.2.7 États-Unis d'Amérique

Les États-Unis d'Amérique sont un acteur crucial des questions touchant le respect de la vie privée dans le monde en raison non seulement de leur poids et de leur importance en général au niveau mondial, mais aussi de leur écrasante domination en termes d'entreprises fournissant des services Internet. De fait, parmi ces entreprises qui sont désormais connues de tous dans le monde – telles que Google, Facebook, Yahoo!, YouTube, Twitter et Wikipedia – presque toutes sont basées aux États-Unis d'Amérique.

Les États-Unis d'Amérique ont une longue et riche histoire en matière de protection de la vie privée, caractérisée par des initiatives législatives déterminantes et souvent innovantes. Cependant, face à cela, il y a aussi une très forte conception de la liberté d'expression, y compris dans le domaine commercial, qui s'est trouvée en opposition avec le souci de protection de la vie privée dans bien des cas. De plus, les responsables de l'élaboration des lois se sont montrés réticents à légiférer spécifiquement sur les questions de confidentialité sur l'Internet, de peur de compromettre l'énorme vitalité du commerce en ligne et/ou de créer un régime de régulation impraticable. Cela a conduit à un cadre juridique global intéressant, qui dans certains domaines est mondialement à la pointe tandis que dans d'autres, et surtout dans le domaine de la protection des données, il ne l'est certainement pas.

Il n'y pas dans la Constitution des États-Unis de garantie directe du respect de la vie privée, bien qu'un droit limité ait été établi à partir de diverses dispositions de la Constitution. L'élément le plus important est l'interprétation donnée au Quatrième Amendement – lequel protège contre les perquisitions et les saisies déraisonnables – pour conclure à un droit à la protection de la vie privée contre l'État, comme l'a fait la Cour suprême des États-Unis en 1967 dans l'affaire Katz c. États-Unis[279]. L'idée de base ici est celle d'une sphère dans laquelle les personnes comptent sur leur intimité,

---

277 Note 207, p. 11.

278 Voir par exemple Orantes, J., Cruz, C. and Morales, P., "Legal Update: Decree Enacting the Federal Law for Protection of Personal Data in Possession of a Person, and Amending Paragraphs II and VII of Article 3, and Article 33, as Well as the Heading of Chapter II, of the Second Title, of the Federal Law of Transparency and Access to Public Governmental Information", disponible à l'adresse http://www.theworldlawgroup.com/files/file/docs/Mexico%20DP.pdf, et Blackmer, S., "Mexico's New Data Protection Law", 28 juillet 2010, disponible à l'adresse http://www.infolawgroup.com/2010/07/articles/data-privacy-law-or-regulation/mexicos-new-data-protection-law/.

279 389 U.S. 347 (1967).

qui comprend à la fois une dimension subjective (à savoir une attente effective) et une dimension objective (à savoir une attente raisonnable). Le fait que cet aspect du droit est fondé sur le Quatrième Amendement empêche d'étendre son application, sur le modèle de l'article 8 de la Convention européenne des droits de l'homme, aux acteurs privés. Il y a eu de nombreuses décisions judiciaires invoquant ces règles. Dans une affaire récente, la Cour suprême des États-Unis a statué que la pose d'un appareil GPS dans un véhicule équivalait à une perquisition, et relevait donc des règles applicables aux perquisitions (exigeant normalement un mandat)[280].

Le délit civil d'ingérence dans la vie privée, qui confère un droit d'agir en justice contre les acteurs privés comme publics, est reconnu en droit depuis plus d'un siècle, et ce aujourd'hui dans presque tous les États. Quatre actions en justice différentes sont généralement admises, permettant de contester l'immixtion déraisonnable dans l'intimité d'une personne, l'appropriation du nom ou de l'image d'autrui, la représentation publique d'une personne sous un jour trompeur et la publicité déraisonnable donnée à la vie privée d'une personne[281].

La Loi sur la vie privée de 1974 institue un système de protection, mais seulement pour les autorités publiques. Les organes privés sont pour la plupart libres de se fixer des normes en ce domaine[282]. À bien des égards, les valeurs et principes de base de la protection des données qui sous-tendent la Loi sur la vie privée sont similaires à ceux de la Directive de l'UE sur la protection des données en dépit de la grande différence de leurs champs d'application[283]. Cependant, les arrangements institutionnels sont très différents. Ainsi, il n'y a pas d'autorité de contrôle indépendante pour la protection des données comme l'exige la Directive de l'UE. Le Bureau de la gestion et du budget (OBM) joue un rôle beaucoup plus limité en matière de définition de la politique à suivre.

Outre ces deux systèmes centraux concernant la protection de la vie privée, il y a aux États-Unis d'Amérique un grand nombre de dispositifs légaux qui sont centrés sur divers secteurs et domaines d'intérêt. La Loi de 1986 sur la confidentialité des communications électroniques (ECPA), qui a essentiellement introduit dans l'ère de la communication en ligne la législation sur les écoutes téléphoniques, assure la protection des communications électroniques. Elle est divisée en trois parties, connues sous les appellations de Loi sur les écoutes téléphoniques, Loi sur les communications stockées et Loi sur le registre des traitements. En gros, la première partie assure la confidentialité des communications quand elles sont en transit et la deuxième, comme son nom l'indique, celle des communications stockées. La troisième interdit de suivre les messages entrants et sortants. Il est possible de déroger à toutes les trois pour diverses raisons, et la première assure la protection la plus forte de la confidentialité. La Loi de 2002 sur la sécurité intérieure (la loi PATRIOT

---

280 United States v. Jones, No. 10–1259, 23 janvier 2012.

281 Voir Lake v. Wal-Mart-Stores Inc., 30 juillet 1998, Minnesota Supreme Court, C7-97-263. Voir aussi Restatement (Second) of Torts, § 652B-E (1977).

282 Les incidences du délit civil d'ingérence dans la vie privée sur la protection des données ont été limitées. Voir The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, note 207, p. 5.

283 Written Statement of Professor Peter P. Swire Moritz College of Law of the Ohio State University Center for American Progress Submitted to the House Energy & Commerce Committee 15 septembre 2011 "Internet Privacy: The Impact and Burden of EU Regulation". Disponible à l'adresse http://www.americanprogressaction.org/issues/2011/09/pdf/swire_testimony.pdf.

comme elle est communément appelée) a affaibli les protections de la confidentialité dans l'ECPA, notamment en élargissant les pouvoirs d'interception pour raisons de sécurité et d'action répressive.

La Loi Gramm-Leach-Bliley de 1999 facilite le partage des informations entre les institutions financières, tout en établissant des normes spéciales pour garantir une protection appropriée de la confidentialité[284]. La Loi de 1994 sur la protection du droit au respect de la vie privée des conducteurs a été adoptée en réaction à la vente de documents sur les véhicules à moteur comportant quantité de données personnelles sensibles – telles que numéros de téléphone, adresses, détails personnels et informations médicales – qui avait abouti à un certain nombre de crimes retentissants, dont le meurtre d'une actrice célèbre. La Loi de 2006 sur la protection des relevés téléphoniques et de la vie privée définit comme un délit le fait d'utiliser un faux prétexte pour obtenir, acheter ou vendre des relevés téléphoniques personnels, tandis que la Loi de 2003 sur la loyauté et l'exactitude des opérations de crédit a créé certains droits à la protection de la vie privée, par exemple le droit d'obtenir gratuitement un rapport de crédit des bureaux compétents une fois par an. Cette loi était aussi un élément d'une stratégie d'ensemble de lutte contre les usurpations d'identité[285]. La Loi de 1980 sur la protection de la vie privée des enfants en ligne (COPPA) requiert le consentement des parents avant que des informations puissent être collectées auprès d'enfants de moins de 13 ans. Elle exige aussi que les sites Web aient une politique de confidentialité, opérant ainsi en tandem avec une approche d'autorégulation.

La Loi de 2004 sur la lutte contre la pornographie et le marketing non sollicités (Loi CAN-SPAM) a été une tentative de définir des normes pour les spams, bien qu'elle soit largement considérée comme n'ayant guère eu d'impact. Elle n'exige pas le consentement des destinataires des spams, mais elle impose aux expéditeurs l'obligation d'indiquer que le message est une publicité et de fournir une adresse postale valide. Les destinataires ont aussi le droit d'adresser une notification de refus des spams.

Les États-Unis d'Amérique ont jusqu'ici refusé d'adopter des règles sur la conservation des données alignées sur celles qui ont été imposées par la Directive de l'UE sur la conservation des données. Des projets de loi conformes à cette orientation ont été proposés, tels que celui de 2009 visant à ce que l'Internet empêche les adultes de faciliter l'exploitation des jeunes d'aujourd'hui (projet de loi SAFETY), proposé mais jamais adopté. Ce texte aurait obligé les fournisseurs de services de communication à conserver pendant au moins deux ans « tous les documents ou autres informations concernant l'identité d'un utilisateur d'une adresse de réseau temporairement assignée par le service à cet utilisateur »[286].

Outre ces lois fédérales, il y a eu beaucoup d'activités au niveau des États sur la question de la vie privée et de l'Internet[287].

---

284 L'Electronic Privacy Information Center et Privacy International qualifient ces normes de « faibles ». Note 119, p. 1009.

285 Voir http://www.money-zine.com/Financial-Planning/Debt-Consolidation/Identity-Theft-Regulations/.

286 http://www.wired.com/threatlevel/2009/02/feds-propose-st/

287 Certaines de ces activités sont listées à l'adresse http://www.ncsl.org/default.aspx?tabid=13463.

3.2.8 Nigéria

L'article 37 de la Constitution de la République fédérale du Nigéria de 1999 dispose : « L'intimité des citoyens, de leur domicile, de leur correspondance, de leurs conversations téléphoniques et de leurs communications télégraphiques est garantie et protégée ». Cependant, l'article 45 dispose que cela n'invalide aucune loi qui est « raisonnablement justifiable dans une société démocratique (a) dans l'intérêt de la défense, de la sûreté publique, de l'ordre public, de la moralité publique ou de la santé publique, ou (b) dans le but de protéger les droits et libertés d'autrui ». Il y a néanmoins très peu de jurisprudence constitutionnelle sur ces questions qui pourrait donner des indications sur la portée pratique de ces limitations.

Il n'y a pas dans la loi nigériane de protection explicite des immixtions civiles dans la vie privée, mais le moyen de la common law de l'abus de confiance s'applique probablement au Nigéria et peut donc être invoqué pour bénéficier d'une protection au civil[288]. Cependant, comme pour la garantie constitutionnelle, il semble qu'il y ait très peu voire pas de jurisprudence sur la question.

À l'heure actuelle, le Nigéria n'a pas de loi gouvernant spécifiquement l'interception des communications privées. Deux projets de loi sur cette question sont en attente au parlement, à savoir le projet de loi de 2009 sur l'interception et la surveillance, et le projet de loi de 2010 sur les moyens de télécommunications (interception licite des informations)[289]. Aux termes de la Loi sur les communications nigérianes de 2003[290], il est présumé que les communications sont privées, mais la Loi prévoit aussi l'interception des communications. Ainsi, l'article 147 dispose : « La Commission peut décider qu'un titulaire de licence ou une catégorie de titulaires de licences doit mettre en œuvre la capacité de permettre l'interception autorisée des communications, et cette décision peut spécifier les exigences techniques de la capacité d'interception autorisée ». L'article 148 prévoit aussi l'interception des communications en cas d'urgence publique.

Deux autres projets de loi ont été étudiés, concernant spécifiquement la protection des informations sur les ordinateurs et l'Internet, à savoir le projet de loi de 2005 sur la protection de l'infrastructure de sécurité des ordinateurs et des informations critiques, et le projet de loi de 2008 sur la cybersécurité et la protection des informations. L'article 13 du premier texte interdirait l'interception illicite de toute communication mais prévoirait une large autorisation pour les interceptions licites, par exemple à des fins de détection et de prévention de la criminalité. Le deuxième texte interdit de même les interceptions illicites mais oblige les fournisseurs de services à posséder la capacité d'intercepter les communications pour aider les organes chargés de l'application de la loi (articles 16-17)[291].

---

288 Voir Nwauche, E.S., "The Right to Privacy in Nigeria" (2007) 1 Review of Nigerian Law and Practice 63.

289 Pour en savoir plus sur ces deux projets de loi, voir Udo Udoma & Belo-Osagie, Law: Intercepting Private Communications in Nigeria, 7 mars 2012. Disponible à l'adresse http://www.proshareng.com/articles/2406.

290 Disponible à l'adresse http://www.nigeria-law.org/Nigerian%20Communications%20Commission%20Act%202003.htm.

291 Pour en savoir plus sur ces projets de loi, voir Akinsuyi, Nigerian Cyber Crime and Privacy Legislations, Time for Review, 9 août 2010. Disponible à l'adresse file:///Users/toby/Documents/Consultancies/Privacy%20-%20UNESCO/Country/Nigeria.Cyber%20Crime%20law.Webarchive.

La loi nigériane ne comprend pas de régime global de protection des données. L'article 12(4) du projet de loi de 2005 sur la protection de l'infrastructure de sécurité des ordinateurs et des informations critiques prévoit une forme très limitée de protection des données :

> Toutes les données conservées, traitées ou extraites par le prestataire de services sur la demande de tout organe d'application de la loi conformément à tout règlement adopté en application du présent article ne sont utilisées qu'à des fins légitimes. En vertu de la présente loi, l'utilisation des données conservées, traitées ou extraites ne constitue une fin légitime qu'avec le consentement des personnes auxquelles s'appliquent les données, ou si elle est autorisée par un tribunal ayant la compétence juridictionnelle ou par une autre autorité légale.

3.2.9 Afrique du Sud

Avec la fin de l'apartheid en Afrique du Sud, le pays a été confronté à un énorme défi : celui de construire un cadre juridique, sans parler d'un cadre social, politique et économique, pour la démocratie. Certains commentateurs ont estimé qu'en raison de ce contexte historique particulier, les énergies sud-africaines tendaient à se concentrer davantage sur les droits à l'égalité que sur des droits-cadres tels que le respect de la vie privée. Sur le plan juridique au moins, il y a quelque chose de vrai dans cette opinion, car le pays n'a toujours pas adopté de loi sur la protection des données. Il y a néanmoins plusieurs sources légales de protection des données.

La Constitution de la République d'Afrique du Sud de 1996 protège la vie privée à son article 14, dans les termes suivants :

Chacun a droit au respect de sa vie privée, qui comprend le droit de ne pas

(a) subir de perquisition sur sa personne ou son domicile ;

(b) subir de perquisition sur ses biens ;

(c) subir de saisie de ses possessions ;

(d) subir d'atteinte à la confidentialité de ses communications.

Il y a eu beaucoup de décisions judiciaires sur les questions constitutionnelles en Afrique du Sud, y compris dans un certain nombre d'affaires touchant la vie privée[292]. Comme la Cour européenne, la Cour constitutionnelle sud-africaine a élaboré une théorie de l'application horizontale des droits, de façon que les protections constitutionnelles puissent s'appliquer entre les individus aussi bien qu'entre les individus et l'État.

Il n'y a pas de protection spécifique de la vie privée par une loi en Afrique du Sud, mais les tribunaux ont depuis longtemps reconnu un droit d'agir en justice fondé sur le concept général du droit romain de l'actio iniuriarum, à savoir le droit d'agir en justice pour protéger sa propre personne. Ce principe a été interprété comme incluant le droit d'agir contre la

---

292 Voir Burchell, J., “The Legal Protection of Privacy in South Africa: A Transplantable Hybrid”, 13.1 Electronic Journal Of Comparative Law, (mars 2009), p. 11-13.

publication non autorisée de faits personnels (tels qu'une photographie), les ingérences déraisonnables dans la sphère privée et le droit à une identité personnelle.

À l'heure de la rédaction de la présente publication, l'Afrique du Sud n'avait toujours pas de législation globale en matière de protection des données, bien que la question soit officiellement examinée depuis 2000 au moins. Un projet de loi sur la protection des informations personnelles, présenté à l'Assemblée nationale en 2009[293], visait à mettre en place un système similaire, pour l'essentiel, au système européen pour la protection des données personnelles détenues aussi bien par les entités privées que par les entités publiques, avec des règles sur le consentement au traitement, la spécification des finalités, la limitation de l'utilisation à d'autres fins, les restrictions à la conservation, les exigences de notification à la fois à la personne concernée et à l'autorité de contrôle, et les droits d'accès et de rectification attribués à la personne concernée. La Cour constitutionnelle a aussi mis en place un cadre très basique pour la protection des données, fondé sur la protection constitutionnelle de la vie privée[294]. On trouve aussi des droits substantiels à la protection des données personnelles dans le National Credit Act[295], destiné en partie à combattre les anciennes pratiques discriminatoires dans le secteur financier. Ces droits comprennent celui de voir ses « informations confidentielles » traitées de manière confidentielle, utilisées exclusivement dans un but légal et divulguées uniquement à la personne à laquelle elles se rapportent.

Pour ce qui est des communications, la législation essentielle est la Loi sur la régulation de l'interception des communications et la fourniture d'informations relatives aux communications[296]. Cette loi est similaire aux autres lois du même genre, assurant généralement la confidentialité des communications privées et ensuite prévoyant des exceptions pour diverses raisons, en particulier la sécurité et l'action répressive, sous réserve de certaines conditions. La Loi impose aux fournisseurs de services de télécommunications l'obligation de faire en sorte que leurs services soient capables de stocker les informations pertinentes sur les communications et de les intercepter avant de les offrir au public. Elle leur impose aussi l'obligation de stocker les informations, selon les instructions du ministre responsable, durant trois à cinq ans.

3.3 Initiatives d'entreprises

Il est clair que les initiatives d'entreprises doivent jouer un rôle clé dans tout système intégré de protection de la vie privée en ligne. Aux États-Unis d'Amérique, ces initiatives restent le système essentiel de protection des données pour ce qui est des acteurs du secteur privé. Dans les systèmes de style européen, elles sont considérées comme un complément important des règles obligatoires sur le plan interne et elles sont souvent à la base des décisions sur l'« adéquation » s'agissant des transferts de données à des tiers. L'article 27 de la Directive 95/46 appelle les États et la Commission à encourager l'élaboration de codes de conduite à des fins d'autorégulation, et les nouvelles propositions élargissent cette perspective en établissant des mécanismes de certification pour les systèmes d'autorégulation, ainsi que des sceaux et des marques de protection

---

293 Publié au Journal officiel du 14 août 2009.
294 Burchell, note 292, p. 14.
295 n° 34 de 2005.
296 n° 70 de 2002.

destinés à permettre aux usagers de déterminer la qualité de ces systèmes. Dans son avant-propos à une étude indépendante sur les nouvelles orientations de la protection des données en Europe, Richard Thomas, Commissaire à l'information du Royaume-Uni, estime qu'à long terme, l'abandon des règles et le transfert aux exportateurs de données de la responsabilité de la protection des données transférées à des tiers (une forme d'autorégulation) sont peut-être inévitables[297].

Cependant, les critiques ne manquent pas à propos des systèmes d'autorégulation qui, de l'avis de beaucoup, n'ont pas abouti à une protection adéquate de la vie privée des usagers aux États-Unis d'Amérique. Dan Tynan a décrit le problème en recourant à une analogie : « Lorsqu'il s'agit de l'industrie de la publicité en ligne, l'autorégulation ressemble un peu aux codes des pirates dans tous ces films de Johnny Depp : ce sont plutôt des principes directeurs que l'on peut violer chaque fois que le scénario l'exige »[298].

Les initiatives d'autorégulation revêtent diverses formes. Beaucoup de FAI et les plus gros et les plus médiatisés des fournisseurs de services en ligne (OSP)[299], comme Google, Yahoo et Facebook, ont mis au point leurs propres politiques de protection de la vie privée. Google a adopté une nouvelle politique qui est entrée en vigueur le 1er mars 2012[300]. Une autre option consiste pour les entités à former un réseau ou une association avec une politique centrale de protection de la vie privée ou un ensemble de normes. Le respect de cette politique est une condition qu'il faut remplir pour être membre du réseau ou de l'association. C'est l'approche adoptée par des groupes tels que la Direct Marketing Association (DMA)[301] et TRUSTe[302]. Les membres sont autorisés à afficher un sceau ou un certificat attestant leur qualité de membres et leur adhésion aux normes collectives.

Quant au fond, il y a plusieurs approches selon les politiques. La plupart des politiques énoncent certains engagements vis-à-vis des usagers, et beaucoup permettent à ceux-ci de sélectionner certaines options en matière de protection de la vie privée. Ainsi, la page d'accueil de chaque usager de Facebook contient un menu déroulant qui vous offre des options telles que paramètres du compte, confidentialité et déconnexion. Sous la rubrique « confidentialité », vous pouvez empêcher autrui de voir vos contenus, paramétrer d'autres options de visualisation pour vos contenus sur Facebook, etc. Cependant, vous ne pouvez pas contrôler l'utilisation que fait Facebook lui-même de vos données privées, bien que divers aspects de cette utilisation soient couverts par sa politique de confidentialité.

Dans certains cas, les politiques autorisent les usagers à refuser que leurs données soient utilisées à diverses fins, essentiellement de marketing. Ainsi, la Network Advertising Initiative (NAI)[303] offre aux usagers une option d'opt out sur la première page de son site, ce qui vous empêche de voir des publicités dédiées des sociétés membres que vous avez exclues. Pourtant, cela n'empêche pas que des cookies soient placés sur votre

---

297 Voir Robinson, Graux, Botterman et Valieri, Review of EU Data Protection Directive: Summary, note 215, Foreword.

298 "Privacy pirates: Self regulation is a sinking ship", 9 août 2011. Disponible à l'adresse http://www.itworld.com/it-managementstrategy/191917/privacy-pirates-self-regulation-sinking-ship.

299 Les OSP sont des entités qui offrent des services en ligne tels que l'hébergement de sites Web, les services de courriel, les réseaux sociaux, les plates-formes de blog, etc.

300 Disponible à l'adresse http://www.google.com/policies/privacy/.

301 Voir www.the-dma.org.

302 Voir www.truste.org.

303 Voir www.networkadvertising.org/.

ordinateur ou de supprimer des données personnelles des bases de données. Une option plus puissante, utilisée par certains réseaux de reconnaissance faciale, tels que la Digital Signage Federation (DSF)[304] et Point of Purchase Advertising International (POPAI)[305], est fondée sur un régime d'opt in, dans lequel les sociétés membres sont censées obtenir l'adhésion des usagers avant de collecter certains types de données.

Il y a plusieurs raisons structurelles pour lesquelles l'efficacité de l'autorégulation est limitée. Une de ces raisons est que beaucoup de systèmes font porter à l'usager l'essentiel du fardeau. Nombre de politiques de confidentialité sont longues, complexes et très légalistes, et il se peut que les usagers ne les comprennent pas ou ne comprennent pas les options de confidentialité. Même s'ils font l'effort pour les FAI et les OSP qu'ils utilisent régulièrement, ils ne peuvent le faire pour tous les services qu'ils utilisent et qui pourraient être en mesure de collecter des données les concernant. S'efforçant de faciliter la tâche de ses usagers, Google a récemment annoncé qu'il unifie les politiques de confidentialité sur tous ses services, de telle sorte que les usagers ne devront se familiariser qu'avec une seule version[306]. Dans l'immense majorité des cas, les entités se réservent le droit de modifier leurs politiques de confidentialité sans informer les usagers, ce qui crée un obstacle de plus pour ceux-ci.

Un autre problème est que s'il peut y avoir des incitations à agir selon des modalités respectueuses de la vie privée pour certaines sociétés – en particulier les plus grandes et les plus connues – pour beaucoup les incitations sont toutes en sens contraire, vu qu'elles gagnent de l'argent en collectant et en vendant des données personnelles. Il peut être coûteux de mettre en œuvre des politiques de confidentialité rigoureuses. La mise en œuvre de nombreux systèmes est faible, entre autres raisons parce que le contrôle est coûteux et rarement systématique. Enfin, la mise en œuvre d'une politique de confidentialité peut en fait accroître les engagements d'une société car celle-ci peut être tenue pour responsable du non-respect de cette politique[307].

Cependant, de nombreux commentateurs notent divers avantages de l'autorégulation. Elle confie le contrôle et la responsabilité aux entreprises, qui sont souvent les entités les mieux à même de comprendre les risques de la confidentialité et de concevoir des solutions efficaces dans un environnement très complexe et qui évolue très vite. L'autorégulation a plus de chances d'être sensible aux besoins des entreprises et d'offrir la flexibilité dont elles ont besoin, là encore dans le contexte d'un secteur incroyablement dynamique. Autrement dit, l'autorégulation peut aider à protéger les bienfaits économiques et sociaux de l'innovation en ligne.

---

304 Voir www.digitalsignagefederation.org/.

305 Voir http://popai.com/.

306 Voir http://www.google.com/policies/.

307 La Federal Trade Commission (FTC) des États-Unis, par exemple, traite les violations de la politique de confidentialité d'une société comme une pratique commerciale trompeuse, c'est-à-dire illicite. Voir Marsh, "Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet" (2009) 15 Michigan Telecommunications and Technology Law Review 543, p. 555.

Un certain nombre d'idées ont été proposées pour améliorer les systèmes d'autorégulation. Une de ces idées est d'employer la confidentialité dès la phase de conception, ou d'intégrer les systèmes de confidentialité dans la conception même des systèmes de services. C'est sans nul doute une bonne idée, mais elle ne saurait résoudre nombre des problèmes notés plus haut.

Certaines idées de co-régulation seraient peut-être plus efficaces. Certains commentateurs, dont la Federal Trade Commission (FTC) des États-Unis d'Amérique, ont demandé l'imposition d'un système d'exclusion sur le modèle des règles populaires mises en place dans certains pays pour les appels téléphoniques[308]. Ce système permettrait aux usagers de refuser la collecte d'informations concernant leur comportement en ligne à des fins de publicité ciblée. Cela pourrait se faire par exemple en plaçant sur le navigateur de l'usager un paramètre indiquant ses préférences. Une autre possibilité, quoique moins radicale, serait de demander aux sociétés de faire connaître au public les éventuelles violations de leurs politiques de confidentialité. Un commentateur a demandé que les législateurs accordent aux sociétés un délai d'un an pour faire des propositions, et imposent ensuite à toutes les sociétés l'obligation d'appliquer le système le plus efficace[309].

---

308 FTC, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers: Preliminary FTC Staff Report, décembre 2010. Disponible à l'adresse http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

309 Ibid., p. 559-562.

4. CONCLUSIONS – INTERSECTIONS ENTRE LE RESPECT DE LA VIE PRIVÉE ET LA LIBERTÉ D'EXPRESSION

Le droit à la vie privée et le droit à la liberté d'expression entretiennent entre eux des relations complexes. Dans bien des cas, l'exercice du droit à la vie privée sert le droit à la liberté d'expression, comme il sert d'autres droits démocratiques. Pour donner un exemple qui tombe sous le sens, le respect de la vie privée dans le domaine des communications est indispensable à la confiance des personnes qui entreprennent de communiquer, confiance qui est elle-même une condition essentielle du droit à la liberté d'expression.

Dans d'autres cas, toutefois, le droit à la vie privée peut entrer en conflit avec le droit à la liberté d'expression, lorsque par exemple un journal souhaite publier des informations de caractère privé concernant une personnalité politique, parce qu'il considère que c'est dans l'intérêt public. Dans l'exemple déjà cité, des commentateurs ont critiqué le caractère excessif de la protection de la vie privée dans le système français, qui avait empêché les médias et d'autres parties d'enquêter sur des allégations de précédents actes douteux imputés à l'ancien président du FMI Dominique Strauss-Kahn.

Ces relations se manifestent sous des formes à la fois classiques et nouvelles sur l'Internet, comme il ressort des deux exemples donnés plus haut (systèmes de communications en ligne et médias en ligne). De fait, les contraintes ont été considérablement allégées par les énormes changements apportés par l'Internet et les autres systèmes de communication numériques (tels que le téléphone mobile) sur le plan de la liberté d'expression. Ainsi, la capacité de l'État de suivre à la trace les activités des individus grâce à leurs communications a fait un bond spectaculaire du fait des possibilités massivement accrues offertes par les systèmes numériques en matière d'exploration des données.

La présente partie du rapport a pour objet d'étudier plus avant ces relations. On examinera tout d'abord les conséquences négatives pour la liberté d'expression d'une protection insuffisante de la vie privée. Puis on s'intéressera aux tensions entre ces deux droits, en indiquant dans certains cas les menaces qu'une protection excessive de la vie privée fait peser sur la liberté d'expression, et en soulignant simplement les tensions dans d'autres cas.

4.1 Conséquences d’une protection insuffisante de la vie privée pour la liberté d’expression

Les premières tentatives pour protéger la vie privée ont été motivées par les cas d’intrusion de l’État dans les espaces privés, qui continuent de rendre indispensable une solide protection de la vie privée en ligne. Il existe depuis longtemps une tension entre la nécessité d’assurer l’application effective de la loi et le respect de la vie privée, comme en témoignent les innombrables plaintes déposées devant les tribunaux de nombreux pays et devant les tribunaux internationaux des droits de l’homme pour atteinte à la vie privée par des agents de la force publique. Ces affaires ont trait surtout, et pour des raisons évidentes, aux communications numériques, mais elles touchent aussi à un certain nombre de domaines où la confidentialité est une question sensible, comme l’accès aux données bancaires ou relatives au crédit.

Cette tension a gagné en complexité ces dernières années du fait d’un certain nombre d’évolutions. Premièrement, nous l’avons vu, la valeur de l’information disponible, du point de vue de l’action de la force publique, s’est considérablement accrue du fait que les nouvelles technologies captent beaucoup plus de renseignements qu’auparavant à notre sujet, et ce de manière permanente et automatisée, que ces renseignements soient communiqués volontairement, par exemple sur une page de Facebook, pour pouvoir bénéficier de la prestation d’un service, comme l’enregistrement des appels provenant d’un téléphone mobile, ou qu’ils soient recueillis à des fins commerciales, lorsque par exemple on relève nos habitudes d’achats en ligne. L’augmentation rapide de la capacité de traitement des ordinateurs modernes a en la matière un fort effet multiplicateur.

C’est ainsi que les données stockées dans le smartphone d’un utilisateur intensif livrent une véritable profusion d’informations sur ses mouvements, ses appels, etc. De plus, de nombreuses formes de communication permettent aujourd’hui l’enregistrement automatique des messages, qui peuvent être retrouvés au moyen d’une recherche informatique, ce qui en accroît énormément l’utilité à des fins de police. Les applications potentielles des dispositifs de reconnaissance faciale, en particulier lorsqu’elles sont combinées à l’usage de plus en plus omniprésent de caméras de vidéosurveillance, en sont un autre exemple.

Deuxièmement, sur le plan de la réglementation, il est beaucoup plus difficile de contrôler les activités de surveillance qu’avant l’Internet. Dans le passé, la mise sur écoute ou la surveillance des appels téléphoniques étaient soumises à des règles simples, quoique souvent levées à titre de dérogation ou contournées, et pas toujours correctement appliquées dans la pratique. Cette activité nécessitait l’installation ou l’activation d’un matériel spécialisé et la mise en place d’une procédure de surveillance ou d’enregistrement particulière, que l’on compare avec la recherche des données stockées dans un téléphone mobile saisi auprès d’un suspect. Qui plus est, la manière dont l’information privée est interceptée et peut être consultée ne cesse d’évoluer, ce qui complique les efforts de réglementation. À cela s’ajoute la possibilité d’une coopération volontaire des fournisseurs d’accès à l’Internet et de services en ligne avec les forces de l’ordre, sans doute dictée principalement par la politique de confidentialité desdits fournisseurs.

Troisièmement, on observe, même dans les démocraties, une tendance manifeste à instaurer un régime juridique qui facilite l’exploitation de cette information à des fins de maintien de l’ordre public. Elle obéit au désir de lutter contre la criminalité par tous

les moyens disponibles, y compris en mettant à profit le fait que les malfaiteurs font souvent un usage efficace de la technologie, en la mettant en particulier au service du crime organisé et du terrorisme. Toutefois, il n'est pas toujours certain que le souci de protéger la vie privée soit pleinement pris en compte, et beaucoup de ces régimes ont été vivement critiqués par les défenseurs du droit à la vie privée. La Directive de l'Union sur la conservation des données, qui n'a pas été toujours bien accueillie par les cours constitutionnelles nationales, en est un bon exemple. De plus, des systèmes que l'on pourrait mettre en conformité avec les règles en matière de protection de la vie privée là où ces règles sont strictes n'en risquent pas moins de prêter à de graves abus dans les (nombreux) pays où elles le sont moins.

Au risque que la vie privée soit insuffisamment protégée s'ajoute souvent celui d'une faible protection directe de la liberté d'expression, d'où un effet multiplicateur. Dans plusieurs affaires qui ont fait du bruit, les autorités chinoises ont ordonné aux fournisseurs de services en ligne de livrer des données privées, ce qui a permis de sanctionner pénalement des activités qui sont protégées par le droit international au titre de la liberté d'expression.

C'est ainsi que le journaliste chinois Shi Tao a été condamné en 2005 à 10 ans de prison pour avoir divulgué dans un courriel une mise en garde du gouvernement enjoignant la presse de s'abstenir d'évoquer les manifestations de la place Tiananmen de 1989. Yahoo! avait, à leur demande, communiqué aux autorités chinoises les courriels provenant du compte de Shi Tao sur la base desquels ce dernier a été reconnu coupable d'avoir divulgué des secrets d'État[310].

Dans bien des cas, les États ont institué un régime visant spécifiquement à contrôler les activités d'expression sur l'Internet. En Thaïlande, la Loi relative aux infractions dans le domaine de l'informatique de 2007, plus connue sous le nom de Loi sur la criminalité informatique, contient des dispositions réprimant la détention et la diffusion d'informations fausses ou de caractère pornographique, ou d'informations de nature à nuire à l'ordre public ou à la sécurité nationale, y compris le crime de lèse-majesté. Ces dispositions ont été appliquées à maintes reprises depuis l'adoption de la loi[311]. De même, la Loi indonésienne de 2008 sur l'information et les transactions électroniques érige en infraction pénale la dissémination de nouvelles fausses, de matériels diffamatoires et de documents pornographiques[312]. Ces deux lois ont été violemment critiquées par les militants qui défendent la liberté d'expression[313].

---

310 Voir http://www.businessweek.com/stories/2007-11-06/jerry-yang-on-the-hot-seatbusinessweek-business-news-stock-market-and-financial-advice.

311 Voir Tunsarawuth, S. et Mendel, T., Analysis of Computer Crime Act of Thailand (2010). Disponible à l'adresse suivante : http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

312 Loi n° 11/2008. Voir les articles 27 et 28.

313 Pour la Thaïlande, voir Analysis of Computer Crime Act of Thailand, note 312, et pour l'Indonésie, AJI, Building the Fortress of Freedom (2009), fichier disponible auprès de l'auteur.

4.2 Tensions entre liberté d'expression et respect de la vie privée

La question des tensions entre liberté d'expression et protection de la vie privée en ligne est beaucoup plus complexe et a des prolongements plus variés que celle des conséquences d'une protection insuffisante du droit à la vie privée sur la liberté d'expression. Si cette dernière a généralement sur la vie privée des incidences évidentes (et souvent reconnues) que l'on tente de justifier par la nécessité supérieure de faire respecter la loi, l'important ici devient la question même de savoir ce qui constitue la sphère privée. Comme on l'a noté plus haut, des tribunaux tant nationaux qu'internationaux ont refusé de donner une définition claire de la vie privée, mais l'approche adoptée par les juridictions des États-Unis d'Amérique, dans laquelle entrent à la fois des éléments subjectifs (attentes effectives) et des éléments objectifs (attentes raisonnables) ne manque pas de mérites.

Le champ ainsi défini par cette conception de la vie privée acquiert une grande importance dans certains cas où la liberté d'expression est en jeu. Par exemple, un ministre de la défense qui dîne dans un restaurant en privé, mais avec un négociant en armes étranger, peut-il raisonnablement s'attendre à être protégé par le droit au respect de la vie privée ? Et qu'en est-il lorsqu'un premier ministre est invité au mariage d'une célébrité ? Des réponses différentes pourront être apportées à ces questions selon les pays, avec des conséquences importantes pour les médias qui souhaitent rendre compte de telles activités.

Cette problématique doit être considérée aussi à la lumière des difficultés fondamentales auxquelles la protection de la vie privée se heurte dans l'univers des réseaux en ligne, et des types de mesures réglementaires qu'elles ont suscitées. Parmi les obstacles considérables à toute tentative de réglementation dans ce domaine figurent :

- Un modèle d'affaires dominant qui implique dans la pratique l'échange ou la cession de données confidentielles en contrepartie de services gratuits.
- Dans bien des cas, des modèles de prestation de services qui impliquent aussi la communication d'informations privées, soit comme condition fondamentale de la prestation (par exemple, sur Facebook), soit comme moyen d'améliorer l'efficacité (cas des outils permettant d'optimiser la recherche sur la base des préférences de l'utilisateur).
- Un environnement résultant de ce qui précède où, quelles que soient les éventuelles incitations, telles que la pression exercée par l'opinion publique sur certaines entreprises commerciales pour qu'elles respectent la vie privée, il est impossible ou presque d'obtenir cela d'un grand nombre d'autres entreprises.
- Une situation générale qui rend presque impossible pour les utilisateurs de donner leur acceptation éclairée des règles de confidentialité du fait, entre autres choses, de la complexité intrinsèque de ces règles, de la quantité considérable d'applications différentes qui sont utilisées et de l'absence d'intérêt ou de la méconnaissance apparentes de la plupart des utilisateurs à cet égard, voire de leur acceptation de la contrepartie susmentionnée.

- Les difficultés inhérentes à la protection du droit au respect de la vie privée, dues notamment à l'incroyable fluidité de l'information et au fait qu'on ne peut plus jamais récupérer ce qui a été « lâché » dans le cyberespace.

Il existe des différences marquées dans les mesures réglementaires, en particulier de protection des données, adoptées aux États-Unis d'Amérique (et dans les pays dotés d'un cadre similaire), d'une part, et en Europe (et dans les pays qui suivent son approche), d'autre part. Les États-Unis d'Amérique, où sont basés bon nombre des principaux fournisseurs de services en ligne de la planète, sont pour l'essentiel adeptes du « laisser-faire », l'action réglementaire de l'État ne s'exerçant que dans certains secteurs, avec sans doute pour effet que les acteurs privés n'offrent qu'une protection insuffisante. L'Europe, en revanche, a fait preuve d'un relatif interventionnisme, dont on a critiqué la trop grande rigidité, l'inadéquation avec les réalités de l'industrie et l'inefficacité dans la pratique (pour ce qui est par exemple du consentement concernant la collecte et l'utilisation des données), et la tendance, en partie pour faire taire ces critiques, à ménager une trop grande latitude dans l'application des nombreuses exceptions et clauses de récupération des données.

La principale interface entre ces deux approches est le programme de certification fondé sur les Principes internationaux de la sphère de sécurité (International Safe Harbor Privacy Principles Certification Program), en vertu duquel les sociétés basées aux États-Unis d'Amérique qui offrent une protection adéquate sont certifiées par l'Union européenne. On a reproché à ce système de ne pas garantir une protection des données privées du niveau des normes européennes, ce qui semble être manifestement le cas, entre autres faute de recours effectifs. Cela étant, il est clair que l'Union européenne a tout intérêt à certifier les fournisseurs de services en ligne ; on la voit mal refuser de certifier des sociétés telles que Facebook ou Google.

S'agissant des incidences particulières sur la liberté d'expression, on peut distinguer un certain nombre d'aspects, comme suit.

4.2.1 L'intérêt général

Un principe bien établi en droit international veut qu'en cas de conflit entre la liberté d'expression et la protection de la vie privée, il convient de considérer le bien public, ou tout autre critère analogue, pour décider de l'intérêt qui prévaut. Ce principe a été, par exemple, clairement affirmé dans les deux affaires Von Hannover c. Allemagne jugées par la Cour européenne des droits de l'homme[314].

La mise en balance, du point de vue de l'intérêt général, du droit à la protection de la vie privée avec le droit à la liberté d'expression est pertinente dans deux cas d'espèce principaux. Premièrement, comme c'était le cas dans l'affaire Von Hannover, la question se pose lorsque l'information, bien que de nature privée, est accessible aux médias, mais que sa plus large diffusion est considérée aux termes du droit national comme exposant la vie privée à une publicité déraisonnable (ou causant quelque autre préjudice connexe). En de pareils cas, la défense de l'intérêt public, qu'elle soit présentée comme un élément

---

314 24 juin 2004, Requête no. 59320/00 et 7 février 2012, Requêtes no. 40660/08 et 60641/08. La Cour européenne s'est davantage référée à la question des débats sur les questions d'intérêt général, mais il semble que l'idée soit pour l'essentiel la même, quoique adaptée aux faits de l'espèce.

du droit à liberté d'expression ou comme faisant partie intégrante des règles régissant la protection de la vie privée, est essentielle. Ainsi, dans la seconde affaire Von Hannover, la Cour européenne a dit que la publication d'informations par ailleurs privées constituait une intrusion justifiée dans la vie privée (ou une activité protégée en vertu du droit à la liberté d'expression), essentiellement parce que les relations entre le « souverain régnant de la Principauté de Monaco », alors malade, et des membres de sa famille étaient un sujet de préoccupation légitime du public. Malheureusement, ce primat de l'intérêt public n'apparaît pas ou n'est pas clairement énoncé dans la législation de nombreux pays.

Deuxièmement, il doit être tenu compte de l'intérêt général lorsque l'on applique l'exception au titre du respect de la vie privée au droit d'accès à l'information détenue par les pouvoirs publics (droit à l'information). Ainsi, dans une Déclaration commune adoptée en 2004,[315] le Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression, le Représentant de l'OSCE chargé des médias et le Rapporteur spécial de l'OEA pour la liberté d'expression ont noté ce qui suit :

> Le droit d'accès devrait être assorti d'un ensemble limité et soigneusement étudié d'exceptions visant à protéger des intérêts supérieurs publics et privés, notamment le respect de la vie privée. Les exceptions ne devraient être appliquées que lorsqu'il y a risque d'atteinte grave à l'intérêt protégé et que cette atteinte est supérieure à l'intérêt que représente l'accès à l'information pour le public.

De même, une Recommandation de 2002 du Comité des Ministres du Conseil de l'Europe[316] contient le Principe IV (2) ci-après :

> L'accès à un document peut être refusé si la divulgation des informations contenues dans le document porte ou est susceptible de porter préjudice à l'un ou à l'autre des intérêts mentionnés au paragraphe 1, à moins qu'un intérêt public supérieur ne justifie la divulgation.

Bon nombre des lois sur le droit à l'information prévoient une exception au droit à la vie privée en vertu du primat de l'intérêt général, mais beaucoup ne le font pas.

Les tribunaux internationaux ont donné quelques indications sur la manière dont doit s'opérer la mise en balance de la liberté d'expression avec le droit à la vie privée. Ils ont dit clairement qu'il existe une très forte présomption en faveur de la liberté d'expression, que la notion d'intérêt public dans ce contexte doit être comprise de manière stricte et que lorsque l'intérêt général commande de rendre des informations publiques, le droit à liberté d'expression prend normalement le pas sur le droit à la vie privée. La raison tombe sous le sens : le droit à la liberté d'expression est une condition fondamentale de la démocratie, et les commentaires touchant des questions d'intérêt public, qui sont publiés pour le bénéfice de tous les membres de la société, doivent être protégés quand bien même ils porteraient atteinte à la vie privée d'un individu.

---

315 Adoptée le 6 décembre 2004. Disponible à l'adresse suivante : http://documents-dds-ny.un.org/doc/UNDOC/GEN/G06/100/27/pdf/G0610027.pdf?OpenElement (Annexe I).

316 Recommandation R(2002)2 du Comité des Ministres aux États membres sur l'accès aux documents publics, 21 février 2002 : http://www.coe.int/t/dghl/standardsetting/media/doc/H-Inf(2003)003_fr.pdf.

L'affaire Mosley c. Royaume-Uni avait trait à la publication de photographies privées de Max Mosley, alors Directeur de la Fédération internationale de l'automobile, se livrant à des activités à caractère sexuel sous le titre « Le patron de la F1 participant à une sinistre orgie nazie avec cinq prostituées ». Mosley finit par avoir gain de cause devant les tribunaux britanniques, en partie parce que le journal s'était trompé en évoquant une soirée sur le thème nazi, ce qui en aurait fait une affaire publique. Une requête en injonction provisoire tendant à empêcher toute nouvelle publication des documents avait auparavant été rejetée ; le plaignant ne l'avait présentée qu'après la publication initiale des photographies et alors que le préjudice était déjà causé pour l'essentiel. Mosley fit appel devant la Cour européenne des droits de l'homme, en arguant que le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord avait bafoué son droit au respect de la vie privée en n'ordonnant pas aux journaux qui se proposaient de publier des documents attentatoires à la vie privée de notifier les personnes concernées de façon qu'elles aient la possibilité de s'opposer par voie de justice à la publication initiale des documents (ce que Mosley n'avait pas fait).

La Cour européenne rejeta cet argument. Dans son arrêt, où elle commentait les principes fondamentaux, elle déclara, entre autres choses :

> La Cour réaffirme également qu'il convient d'opérer une distinction entre un reportage relatant des faits – même controversés – susceptibles de contribuer à un débat d'intérêt général dans une société démocratique et le fait de formuler des allégations sordides concernant la vie privée d'une personne. Dans le premier cas, le fait que la presse joue son rôle essentiel de « chien de garde » comme elle en a le devoir dans une démocratie milite fortement pour une conception étroite de toutes limites imposées à la liberté d'expression [références omises][317].

Dans les deux affaires Von Hannover, la Cour européenne des droits de l'homme a également précisé la question de la mise en balance du droit à la vie privée et du droit à la liberté d'expression (voir pour plus de détails l'encadré XIII). Dans ces affaires aussi, la Cour a semblé suggérer que lorsque la publication répondait à l'intérêt public, le droit à la liberté d'expression devait normalement l'emporter. Elle s'est fondée, entre autres choses, sur sa position de longue date selon laquelle, concernant la presse, « il ... incombe néanmoins [à celle-ci] de communiquer, dans le respect de ses devoirs et responsabilités, des informations et des idées sur toutes les questions d'intérêt général »[318].

C'est la même approche qui a souvent été appliquée s'agissant du poids relatif du droit à la liberté d'expression et du droit au respect de la réputation, au sujet duquel les tribunaux internationaux ont là encore estimé très important d'accorder une grande liberté de parole sur les questions d'intérêt général. Ainsi, dans l'affaire Herrera-Ulloa c. Costa Rica, qui portait sur une condamnation au pénal pour diffamation, la Cour interaméricaine des droits de l'homme a déclaré ce qui suit :

> Dans ce contexte, il est logique et approprié de considérer que les déclarations concernant des fonctionnaires et autres personnes exerçant des fonctions d'un caractère public doivent, conformément au paragraphe (2)

---

317 10 mai 2011, Requête no. 48009/08, par. 114.
318 Von Hannover c. Allemagne, 24 juin 2004, Requête no. 59320/00, par. 58.

> de l'article 13 de la Convention, bénéficier d'une certaine tolérance dans le cadre du débat général sur les questions d'intérêt public qui est essentiel au bon fonctionnement d'un système véritablement démocratique[319].

Cette idée est également défendue à l'article 12(4) de la loi sur les droits de l'homme du Royaume Uni de Grande-Bretagne et d'Irlande du Nord de 1998, qui dispose :

> Le tribunal accorde une attention particulière à l'importance du droit à la liberté d'expression énoncé dans la Convention et, lorsque l'action intentée a trait à des documents qui, aux dires du défendeur, ou de l'avis du tribunal, sont de nature journalistique, littéraire ou artistique (ou à des actes en rapport avec de tels documents),
>
> (a) à la mesure dans laquelle
>
> (i) les documents ont été ou sont sur le point d'être mis à la disposition du public, ou
>
> (ii) leur publication est, ou serait, dans l'intérêt général ;
>
> (b) à toute disposition pertinente en matière de protection de la vie privée.

4.2.2 Protection de la vie privée et protection des données

Il existe d'importantes différences entre les règles visant à protéger la vie privée en elle-même et celles qui ont pour objet la protection des données. Les secondes sont conçues pour répondre aux problèmes particuliers qui peuvent surgir lorsque des organismes publics ou privés entreprennent de collecter systématiquement des données concernant des individus. Protection des données et protection de la vie privée se recouvrent en grande partie, et les tribunaux internationaux ont considéré que certains éléments des régimes de protection des données étaient couverts par le droit au respect de la vie privée.

Dans le même temps, les règles relatives à la protection des données diffèrent de celles qui régissent la protection de la vie privée, du point de vue du champ d'application comme des principes de fond. Les premières s'appliquent à toutes les données d'identification personnelle, tandis que les secondes, même si elles n'ont jamais fait l'objet d'une définition exhaustive, ne s'appliquent qu'à une catégorie restreinte d'informations, à savoir normalement celles dont une personne peut raisonnablement attendre qu'elles demeurent privées. Cela étant, les règles de protection des données ont une portée plus limitée dans la mesure où, de manière générale, elles ne s'appliquent qu'aux données ou ensembles structurés de données faisant l'objet d'un traitement informatisé, alors que les règles de protection de la vie privée peuvent s'appliquer à tout type d'information (indiquant, par exemple, qu'une personne a dîné en compagnie d'une autre dans un restaurant).

En soi, ce n'est pas un problème. Toutefois, à la différence des interprétations juridiques du droit au respect de la vie privée, les règles de protection des données ne reconnaissent pas le primat de l'intérêt général. La Directive 95/46 de l'Union européenne[320], par exemple, autorise le traitement des données, ainsi que leur communication, au nom de

---

319 2 juillet 2004, Série C no. 107, par. 128.
320 Voir note 205.

l'intérêt public dans certains cas particuliers[321], mais non en tant que règle générale. Ce même régime autorise aussi les États à accepter une exception aux règles principales lorsque les données sont traitées à des fins journalistiques, artistiques ou littéraires, comme l'exige le respect du droit à la liberté d'expression. Là encore, il est à noter que ce principe a une portée limitée et ne s'appliquerait pas à de nombreuses formes d'expression (y compris sans doute le présent rapport).

Dans la pratique, cette question est le plus problématique quand le droit à l'information est en jeu. Dans nombre de pays, on lie entre elles dans les dispositions de la loi, ou on confond au stade de l'application, les règles de protection des données et l'exception en vertu du respect de la vie privée à la législation relative au droit à l'information.

Une meilleure pratique en matière de législation du droit à l'information consiste à inclure une restriction destinée à protéger la vie privée qui indique clairement que toutes les données d'identification ne sont pas couvertes. Ainsi, l'article 34 de la Loi de promotion de l'accès à l'information adoptée par l'Afrique du Sud[322] établit une exception qui vise à prévenir la « divulgation irraisonnable d'informations personnelles au sujet d'un tiers ». De telles lois incluent aussi des exceptions à l'exception au titre du respect de la vie privée, par exemple lorsque l'intéressé a donné son consentement, lorsque l'information est déjà publique ou lorsque l'information a trait aux fonctions officielles d'un agent public[323]. Enfin, ces lois énoncent clairement le primat de l'intérêt général sur toutes les exceptions, de telle sorte que même des informations privées peuvent être divulguées lorsqu'il en va de l'intérêt public. Toutes ces règles sont clairement en accord avec l'interprétation par les tribunaux internationaux du droit à la liberté d'expression, sur lequel repose le droit fondamental à l'information.

Dans le même temps, la législation de nombreux pays, qu'elle impose ou non de telles limites à l'exception au droit d'accès au nom de la protection de la vie privée, ne précise pas clairement la relation entre les règles protégeant le droit à l'information et celles qui régissent la protection des données, et la pratique dominante, au moins dans quelques pays, est d'appliquer les secondes lorsqu'il s'agit de données personnelles. En Inde, en revanche, le projet de loi sur la protection de la vie privée, qui tend à instituer un système général de protection des données, n'affecterait pas le régime établi par la Loi sur le droit à l'information adoptée en 2005.

4.2.3 Champ de la protection et juridiction compétente

Certains pays ont tenté d'étendre le champ de la protection de la vie privée d'une manière qui pourrait avoir des effets négatifs sur la liberté d'expression. Tel est par exemple le cas, évoqué plus haut, de l'Argentine, où les règles visant à protéger la vie privée ont été appliquées aux moteurs de recherche au motif que ces derniers livraient accès à des données portant atteinte à la vie privée. Autre exemple, celui de l'Italie, où trois responsables de Google ont été condamnés à des peines de six mois de prison avec sursis pour avoir diffusé sur Google Videos une séquence montrant des brimades infligées à un jeune autiste, alors même que cette vidéo avait été promptement retirée après dépôt d'une plainte officielle. Richard Thomas, ancien Commissaire à l'information

321 Voir articles 7(e), 8(4) et 26(1)(d).
322 Loi no. 2, 2000. Disponible à l'adresse suivante : http://www.gov.za/gazette/acts/2000/a2-00.pdf.
323 Voir article 34 de la loi de l'Afrique du Sud, ibid.

du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, qualifia le jugement de « ridicule »[324], et Google fit immédiatement appel.

Dans l'un et l'autre cas, on pouvait raisonnablement faire valoir que les auteurs premiers des documents étaient coupables d'atteintes à la vie privée. Néanmoins, si la tendance à rendre les fournisseurs de services en ligne responsables de ce type de situations se généralisait, il deviendrait pour eux presque impossible de continuer à fournir les services importants pour la liberté d'expression qu'ils offrent actuellement.

Dans ces deux exemples, les documents incriminés (concernant des célébrités en Argentine et un jeune garçon italien) relevaient clairement de la juridiction des tribunaux saisis. Mais le risque existe que les plaignants choisissent à leur guise les tribunaux devant lesquels porter les affaires d'atteinte à la vie privée, une pratique connue sous le nom de « tourisme de la diffamation » qui a pris des dimensions mondiales. Les tribunaux seraient ainsi saisis en fonction des chances de succès qu'ils offrent aux plaignants, sans grand rapport avec leur compétence juridictionnelle. C'est privilégier le plus petit dénominateur commun en matière d'équilibre entre le droit au respect de la vie privée et le droit à la liberté d'expression.

Un cas extrême en est l'action en diffamation intentée à l'encontre de Rachel Ehrenfeld, actrice basée à New York, par Sheikh Khalid bin Mahfouz, un richissime homme d'affaires saoudien qu'elle avait mis en cause dans son livre Funding Evil : How Terrorism is Financed and How to Stop It (Le financement du mal : comment le terrorisme est financé et comment y mettre fin). L'affaire fut portée devant les tribunaux du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, alors même que 23 exemplaires seulement du livre avaient été vendus dans ce pays, et un jugement fut rendu par défaut en faveur de bin Mahfouz (Ehrenfeld s'était refusée à présenter sa défense)[325].

4.2.4 Publicité des décisions judiciaires

Les préoccupations relatives au respect de la vie privée, et autres questions connexes, commencent à influer sur la manière dont les tribunaux communiquent l'information relative à leurs travaux. C'est un domaine dans lequel il y a très peu de normes établies, et où la décision est souvent laissée à chaque tribunal ou système judiciaire. Si le principe de la transparence est bien établi, y compris dans le droit international relatif aux droits de l'homme, il a été en général appliqué principalement à l'accès aux affaires traitées par les tribunaux, plutôt qu'aux documents judiciaires.

Dans certains pays, les tribunaux sont pleinement visés par les lois générales sur le droit à l'information, et c'est ce régime qui détermine la transparence à laquelle ils sont tenus en ce qui concerne les documents. Dans beaucoup, cependant, ces dispositions n'ont qu'une portée limitée et ne concernent parfois que les fonctions administratives des tribunaux, et dans certains cas excluent totalement la fonction judiciaire.

---

324 Voir http://news.bbc.co.uk/2/hi/8533695.stm.

325 Voir Mapping Digital Media: Reference Series No. 1 : Online Media and Diffamation (2011, Open Society Foundations). Disponible à l'adresse suivante : http://www.soros.org/sites/default/files/online-media-and-diffamation-20110503.pdf.

Même si les organismes publics ont presque tous tendance à publier un volume croissant d'informations en ligne[326], les préoccupations en matière de protection de la vie privée ont conduit certains tribunaux, surtout aux États-Unis d'Amérique, où cette pratique de la diffusion en ligne des documents judiciaires est la plus répandue, à faire machine arrière. C'est une chose par exemple de publier un jugement rendu au pénal dans un journal local, et c'en est une autre de le diffuser en ligne, après quoi il restera accessible de manière permanente, risquant ainsi de compromettre la réinsertion professionnelle et sociale de la personne condamnée.

Face à ces préoccupations, la Floride, autrefois à l'avant-garde dans ce domaine, a imposé un moratoire sur les efforts visant à étendre l'accès en ligne[327]. Une action intentée en Californie visait un homme d'affaires qui s'était procuré pour les vendre des informations sur des individus ayant fait l'objet de poursuites au pénal. La question était de savoir s'il était en droit d'accéder à des fichiers électroniques regroupant des informations sur de tels individus, sans avoir à se rendre physiquement auprès des tribunaux concernés pour obtenir ces documents. Le tribunal a estimé que c'était le fait même que l'information était de nature électronique qui présentait des risques sur le plan du respect de la vie privée.

Il existe une existence d'ordre qualitatif entre le fait d'obtenir des informations auprès d'un greffe particulier ou au sujet d'une personne particulière, et le fait d'obtenir des informations auprès d'un greffe au sujet de toute personne faisant l'objet de poursuites au pénal devant un tribunal national. (…) C'est la nature agrégée de l'information qui en fait l'utilité pour le défendeur ; c'est cette même qualité qui en rend la diffusion dangereuse au regard du droit constitutionnel[328].

---

326 Comme le demandent de vastes mouvements internationaux, tels que l'Open Government Partnership (OGP). Voir : http://www.opengovpartnership.org/.

327 Voir Open Society Justice Initiative, Report on Access to Judicial Information, mars 2009. Disponible à l'adresse suivante : http://www.right2info.org/resources/publications/Access%20to%20Judicial%20Information%20Report%20R-G%203.09.DOC/view.

328 Westbrook v. County of Los Angeles (1994) 27 Cal. App. 4th 157, p. 165.

5. RECOMMANDATIONS PRATIQUES

Tout au long de ce rapport, nous nous sommes livrés à un examen approfondi de la question de la protection de la vie privée sur l'Internet, considérée du point de vue de la liberté d'expression, en passant en revue les différentes questions que cela soulève, les normes internationales et les pratiques nationales. La présente section contient nos recommandations à l'adresse des États et des sociétés commerciales concernant les meilleures pratiques en matière de respect de la vie privée sur l'Internet, considérées à la lumière du droit international et des politiques nationales, et compte tenu des conflits potentiels avec d'autres droits, en particulier le droit à la liberté d'expression.

La manière classique de résoudre les tensions entre le droit à la vie privée et le droit à la liberté d'expression, tous deux garantis par le droit international, consiste, comme on l'a vu au chapitre précédent, à privilégier dans chaque cas particulier celui de ces deux droits qui sert au mieux l'intérêt général. On observe ainsi une grande tolérance dans le cas d'informations touchant des questions d'intérêt public, qui ont trait par exemple à des personnalités politiques, même si elles constituent par ailleurs une violation de leur vie privée.

L'avènement des régimes modernes de protection des données, qui offrent d'importantes garanties en matière de respect de la vie privée, a introduit une certaine confusion dans l'application du critère susmentionné. Il importe à cet égard de souligner que la protection des données ne se confond pas avec la protection de la vie privée. Les règles de protection des données sont conçues pour prévenir ou corriger d'éventuels abus liés au traitement automatisé d'ensembles de données. Tout en recouvrant en partie le champ des règles de protection de la vie privée, elles s'en distinguent néanmoins. Elles ont une portée plus large dans la mesure où elles s'appliquent à toutes les données d'identification personnelle, tandis que les règles de protection de la vie privée ne s'appliquent qu'aux informations dont on peut raisonnablement s'attendre qu'elles conservent un caractère privé. Et elles sont plus restreintes dans la mesure où elles ne s'appliquent qu'à des ensembles de données, soit en principe ceux qui font l'objet d'un traitement informatisé. Elles ne seraient donc pas d'application dans le cas d'informations détenues par un média qui aurait enquêté sur l'éventuelle corruption d'un fonctionnaire.

Cette distinction est importante parce que, tout en comprenant un certain nombre de règles visant spécifiquement à protéger divers intérêts publics, la plupart des régimes de protection des données ne prévoient pas de véritable primat de l'intérêt général. De ce fait, ils risquent de ne pas toujours assurer le plein respect de la liberté d'expression[329].

---

329 On trouvera une bonne analyse de cette problématique du point de vue de l'accès à l'information dans Mendel, T. (2012) Facilitating Access to Information for Research Purposes - A Comparative Survey. Belgrade, PNUD. Disponible à l'adresse suivante : http://www.poverenik.org.rs/en/publications-/studies/1384-facilitating-access-to-information-for-research-purposes-a-comparative-survey.html.

5.1 Dispositions législatives et réglementaires

5.1.1 Dispositions constitutionnelles

- La constitution devrait prévoir une solide protection du droit à la vie privée comme du droit à la liberté d'expression. Il conviendrait notamment que ces deux droits fassent l'objet de garanties positives et, dans l'idéal, que l'État ait une obligation positive de les protéger contre toute interférence privée.
- La constitution ne devrait autoriser que des restrictions limitées du droit à la vie privée comme du droit à la liberté d'expression. Ce régime devrait permettre en cas de conflit entre l'un et l'autre droits d'arbitrer en fonction de ce qui apparaît comme l'intérêt général. En l'absence de fortes considérations contraires, il devrait être interprété comme autorisant un débat public sur les questions d'intérêt général, même si cela impliquait la divulgation d'informations privées.

Élément faîtier du système juridique, la constitution contient le plus souvent un énoncé ou charte des droits de l'homme, dont elle garantit l'exercice. Peut-être faut-il s'étonner qu'une protection directe du droit à la vie privée ne figure pas expressément dans la constitution de nombre des pays auxquels nous nous sommes intéressés plus haut, même si, dans bien des cas, les tribunaux l'ont interprétée comme si tel était le cas dans leurs décisions.

Néanmoins, il est manifestement préférable que le droit à la protection de la vie privée soit inscrit dans la constitution. Cela étant, amender la constitution est souvent, et à juste titre, un exercice complexe, qui ne doit être entrepris qu'après une large consultation de l'opinion publique, de façon à avoir l'assurance que le texte reflète la volonté de la majorité et bénéficie d'un soutien massif de la nation.

La notion de protection de la vie privée a longtemps été déterminée par l'état de la technique. Si, dans son sens le plus évident, elle implique des limites imposées à l'invasion de l'espace physique et la protection du domicile et des biens personnels, la question du contrôle des informations relatives aux personnes privées se pose inévitablement dans le cadre de l'ajustement aux incidences des technologies de la communication.

Certaines constitutions énoncent, souvent de manière non exclusive, le contenu du droit au respect de la vie privée. Ainsi, la Constitution de l'Afrique du Sud inclut expressément le droit d'être protégé contre la fouille du domicile ou des biens, la saisie des biens ou l'interception des communications[330]. De même, la Constitution du Nigéria mentionne le caractère privé du domicile, de la correspondance et des autres formes de communication[331]. Tout en ayant le mérite de la clarté, ces énumérations présentent le risque que les éléments qui n'y sont pas inclus – par exemple la présomption raisonnable d'être protégé contre toute intrusion dans l'espace privé – soient considérés comme exclus. Lorsqu'il est fait expressément mention des communications, il doit être indiqué clairement que tous les types de communications sont visés, y compris toutes formes de communication sur l'Internet (courriels, messages publiés sur les sites de réseaux sociaux ou de groupes de discussion en ligne, achats, recherches, traces laissées sur les sites visités, etc.).

---

330 Article 14.
331 Article 37.

Il serait peut-être préférable que la constitution mentionne simplement le respect de la vie privée au sens large, comme le font les principaux instruments internationaux. La constitution pourrait aussi faire référence aux principaux attributs généraux de la vie privée, par exemple comme comprenant des éléments tant subjectifs qu'objectifs, ou au concept d'autonomie de la personne, qui est au fondement de la notion de vie privée. Ces attributs pourraient être expressément énoncés dans la constitution ou laissés à l'appréciation des tribunaux.

En droit international, et dans le droit constitutionnel de nombreux pays, la protection des droits de l'homme s'entend contre tous éventuels abus de pouvoir de la part de l'État, plutôt que d'acteurs privés. Néanmoins, le droit international et de nombreuses constitutions reconnaissent l'existence d'une obligation positive de l'État de protéger les individus contre les atteintes à leurs droits causées par des acteurs privés, ce que l'on appelle parfois l'effet horizontal des droits. Étant donné que ces droits peuvent être menacés aussi bien par l'État que par des acteurs privés, il s'agit là d'une importante dimension de la protection globale de la vie privée.

Le droit à la vie privée n'est pas un droit absolu, comme il ressort clairement du présent rapport. Il peut être limité, entre autres choses par les nécessités du maintien de l'ordre ou par les droits d'autrui (notamment le droit de rechercher, obtenir et communiquer des informations et des idées, soit ce qui constitue la liberté d'expression). Les garanties offertes par la constitution doivent en tenir compte. Pour préserver les fondements du droit à la vie privée, la constitution doit tracer des limites claires à toute restriction de ce droit.

Le Pacte international relatif aux droits civils et politiques est de peu de secours sur ce point, puisqu'il offre simplement une protection contre les « immixtions arbitraires ou illégales dans [l]a vie privée », ce qui n'éclaire guère sur ce qui est ou n'est pas autorisé, et la Convention américaine relative aux droits de l'homme utilise des termes similaires. Plus détaillée, la Convention européenne des droits de l'homme n'admet les restrictions qu'à trois conditions, à savoir qu'elles soient prévues par la loi, qu'elles protègent l'un des droits qui sont énumérés, et qu'elles constituent des mesures nécessaires dans une société démocratique pour la protection de ces droits. Ces conditions sont très proches du critère auquel le Pacte international et la Convention européenne soumettent les restrictions à la liberté d'expression, critère qui s'est révélé offrir une base assez solide pour la protection de ces droits.

La Constitution du Mexique, en revanche, s'étend de manière assez détaillée sur les garanties de procédure en matière de respect de la vie privée, en précisant clairement dans quelles circonstances sont autorisés les mandats de perquisition et les perquisitions, ainsi que l'interception des communications[332]. La Constitution de l'Afrique du Sud prend davantage modèle sur la Convention européenne des droits de l'homme, et indique que les restrictions doivent faire l'objet d'une loi d'application générale, et être « raisonnables et justifiables dans une société ouverte et démocratique fondée sur la dignité humaine, l'égalité et la liberté », eu égards à divers facteurs[333].

332 Article 16.
333 Article 36 (1). voir aussi l'article 45 de la Constitution du Nigéria, de conception similaire.

Il est également important que la constitution assure la protection de la liberté d'expression. En droit international, le régime des exceptions à ce droit est très proche de celui qui s'applique dans la Convention européenne des droits de l'homme au droit à la vie privée. En particulier, il implique un critère en trois points en vertu duquel les restrictions ne sont autorisées que si elles sont prévues par la loi, si elles protègent l'un des intérêts visés et si elles sont nécessaires pour protéger cet intérêt.

Quelle que soit la formulation de tel ou tel régime d'exceptions, il importe que les garanties offertes par la constitution en matière de vie privée comme de liberté d'expression soient conçues pour être compatibles l'une avec l'autre. Nous l'avons vu au précédent chapitre, cela signifie essentiellement qu'en cas de conflit entre les deux droits, c'est l'intérêt général qui doit primer.

5.1.2 Les protections en droit civil

- Le droit civil doit prévoir un recours privé contre les intrusions dans la vie privée, définies (expressément ou à l'appréciation des tribunaux) de manière à couvrir les informations dont ont peut raisonnablement compter qu'elles relèvent de la sphère privée.
- Pour être en accord avec les normes constitutionnelles recommandées ci-dessus, cette règle devrait permettre une mise en balance avec l'intérêt général lorsque des questions de liberté d'expression sont en jeu.
- Le recours devrait offrir aux personnes à la vie privée desquelles il a été porté atteinte une voie appropriée pour obtenir réparation, compte tenu le cas échéant du droit à la liberté d'expression.

La principale voie de recours en matière de protection de la vie privée consiste dans la plupart des pays à intenter une action au civil. On considère en effet que les atteintes à la vie privée, comme à la réputation, sont essentiellement une affaire privée entre les parties, et relèvent donc du droit civil. C'est du reste la manière la plus efficace d'assurer la protection du droit au respect de la vie privée.

Nombreux sont les pays où la loi reconnaît que l'atteinte à la vie privée est un motif spécifique pour engager des poursuites judiciaires. Dans d'autres pays, de telles poursuites s'inscrivent dans le cadre de recours plus généraux. Ainsi, dans les pays de common law, qui appliquent le système juridique en vigueur au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, c'est la divulgation d'informations confidentielles qui est invoquée pour introduire un recours en cas d'atteinte à la vie privée, tandis que dans beaucoup de pays de droit romain, où le système juridique repose sur des codes de lois détaillés, le concept d'*actio iniuiarum* est utilisé à même effet.

De toute évidence, offrir une possibilité de recours pour atteinte à la vie privée est une meilleure pratique, et c'est une obligation en droit international (et dans de nombreuses constitutions)[334]. Pour des raisons de clarté, il est probablement préférable d'offrir une protection expresse de ce droit, même si les tribunaux internationaux admettent que

---

334 Voir, par exemple, Observation générale n°. 16 du Comité des droits de l'homme des Nations Unies, Le droit au respect de la vie privée, de la famille, du domicile et de la correspondance, et le droit d'être protégé contre les atteintes à l'honneur et à la réputation (Article 17), 8 avril 1988.

la possibilité d'intenter une action pour divulgation de données confidentielles peut constituer une protection suffisante[335].

De nombreuses lois sur le droit à la vie privée ne donnent de fait aucune définition de ce droit, et nous avons noté les difficultés que soulevait toute définition précise. Il importe cependant de noter que la protection de la vie privée diffère de la protection des données d'identification personnelle (qui est la norme en ce qui concerne les règles de protection des données). Au lieu de quoi, on trouve dans un certain nombre de juridictions – y compris celles de la France[336], du Canada[337] et de l'Australie[338] – la notion d'attente raisonnable en matière de respect de la vie privée, qui a également été invoquée par la Cour européenne des droits de l'homme[339]. Cette notion semble imposer une solide limitation générale au concept de protection de la vie privée (car en l'absence d'une telle attente raisonnable, il devient alors impossible d'invoquer le caractère privé de tel ou tel document). Nombre des restrictions apportées à la sphère privée dans différentes lois – par exemple lorsque l'intéressé a consenti à la divulgation, lorsque l'information est déjà publique ou lorsqu'elle a trait aux fonctions d'un agent public – peuvent être considérées comme des développements particuliers de l'idée générale d'attente raisonnable en matière de protection de la vie privée.

Aux États-Unis d'Amérique, le délit d'intrusion dans la vie privée offre depuis longtemps déjà une protection d'ordre essentiellement commercial contre l'appropriation du nom ou de l'image. Mais d'autres pays opèrent une distinction entre la vie privée considérée sous l'angle de l'autonomie de la personne et les intérêts commerciaux liés au contrôle exercé sur l'information privée. La question s'est posée au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord dans l'affaire Douglas v. Hello! Ltd, qui portait sur la publication non autorisée de photographies du mariage de Michael Douglas et Catherine Zeta-Jones par le magazine Hello!, alors que les plaignants avaient vendu des droits exclusifs sur cet événement à un autre magazine, à savoir OK!. La Cour d'appel britannique a estimé que, même s'ils avaient consenti à la publication des photos de leur mariage, les plaignants conservaient néanmoins un droit (mineur) sur leur vie privée, en grande partie parce qu'ils avaient un droit de veto sur la publication des images par OK!, droit qu'ils ne pouvaient invoquer contre Hello![340]. La Cour a considéré par ailleurs qu'ils possédaient un intérêt commercial protégé. Il existe des différences marquées entre ces deux types d'intérêts

---

335 Voir Le comte et la comtesse Spencer c. Royaume-Uni, 16 janvier 1998, Requêtes n°. 28851/95 et 28852/95 (Commission européenne des droits de l'homme). Depuis, les tribunaux du Royaume-Uni ont invoqué la législation réprimant la divulgation de données confidentielles pour faire de l'atteinte à la vie privée un motif direct de poursuites judiciaires. Voir Campbell v MGN Ltd [2004] 2 AC 457, par. 51.

336 Schneider c. Sté Union Editions Modernes, 5 juin 1979, Cour d'appel de Paris.

337 Aubry c. Éditions Vice-Versa Inc. [1998] 1 SCR 591, par. 57 et suiv.

338 Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd [2001] HCA 63 (15 novembre 2001), par. 42.

339 Von Hannover c. Allemagne, 24 juin 2004, requête n°. 59320/00, par. 51.

340 Douglas & Ors v Hello Ltd. & Ors [2005] EWCA Civ 595 (18 mai 2005), par. 109. Dans une affaire antérieure portée devant la Cour d'appel au sujet d'une requête en injonction tendant à faire interdire la publication de photographies par le magazine Hello!, le juge Sedley a déclaré : « Si les faits se résumaient à ce que Hello! s'était procuré des photographies d'OK!, OK! aurait des droits de propriété et des recours en droit, mais M. Douglas et Mme Zeta-Jones ne pourraient, selon moi, prétendre à aucune réparation pour une atteinte à leur vie privée à laquelle ils avaient déjà consenti ». Douglas & Anor v Northern And Shell Plc & Anor [2000] EWCA Civ 353 (21 décembre 2000), par. 140.

– respect de la vie privée et valeur commerciale – entre autres choses parce qu'un seul des deux, la vie privée, est protégé par le droit international relatif aux droits de l'homme. Ces différences justifient semble-t-il un traitement différent de ces intérêts au regard du droit.

Une question importante est celle des recours disponibles en cas d'intrusion dans la vie privée, en particulier lorsque des questions touchant la liberté d'expression sont en jeu, comme cela n'est pas rare. Le dédommagement financier est la forme de réparation la plus courante en cas d'atteinte à la vie privée. Dans le droit français, d'autres recours sont possibles, y compris la saisie des documents incriminés, et toute autre mesure qui pourrait être appropriée pour mettre fin à l'infraction. Dans l'affaire Douglas v. Hello! Ltd, la Cour d'appel britannique a rejeté une requête en injonction tendant à faire interdire la publication des photos, entre autres motifs parce que le magazine OK! pouvait poursuivre Hello! en vue d'obtenir un dédommagement commercial, et que les plaignants ne conservaient qu'un intérêt privé limité (ayant vendu l'essentiel de leurs droits privés)[341]. En Argentine, les tribunaux peuvent accorder des dommages-intérêts, ordonner qu'il soit mis fin à l'activité délictueuse et, s'il y a lieu, ordonner la publication du jugement.

Dans le droit international, même lorsqu'une restriction des droits est justifiée, l'imposition de pénalités excessives peut, en elle-même, constituer une atteinte au droit[342]. Il s'ensuit que, même lorsque le droit à la vie privée prime sur le droit à liberté d'expression, l'ampleur des réparations doit tenir compte de ce dernier (en d'autres termes, la réparation doit elle aussi être proportionnée).

5.1.3 Les protections en droit pénal

- Les États devraient instituer des règles pénales d'application sectorielle en matière de vie privée, afin de protéger certaines informations hautement sensibles dans des secteurs tels que les télécommunications et les banques.
- Ces protections ne devraient pas avoir un caractère absolu, et connaître par exemple des exceptions lorsqu'une surveillance des télécommunications est nécessaire à des fins de police, mais leur levée devrait être subordonnée à de strictes conditions de procédure (nécessité en principe d'une ordonnance judiciaire) et de fond (nécessité de prouver que les mesures sont indispensables pour enquêter sur une grave infraction à la loi).
- Il convient d'éviter une interdiction générale, assortie de sanctions pénales, de toute intrusion dans la sphère privée, car elle risque d'entrer en conflit avec le droit à liberté d'expression.

Certain pays – comme la Chine, l'Argentine et les États-Unis d'Amérique – ne prévoient des sanctions pénales pour atteinte à la vie privée que dans des cas limités, en vue essentiellement d'interdire la diffusion de certains types d'information dans des secteurs particuliers (par exemple dans le domaine des télécommunications ou des banques). Outre ces mesures qui tombent sous le sens, divers pays ont adopté des dispositifs

---

341 Douglas & Anor v Northern And Shell Plc & Anor [2000] EWCA Civ 353 (21 décembre 2000), par. 144.

342 Voir, par exemple, Tolstoy Miloslavsky c. Royaume-Uni, 13 juillet 1995, Requête n°. 18139/91 (Cour européenne des droits de l'homme).

pénaux pour lutter contre des problèmes particuliers[343]. Dans certains cas, ces règles de droit pénal ne protègent que l'information détenue par des agents publics, mais elles s'appliquent parfois aussi au secteur privé.

Dans un petit nombre de pays – notamment en France – les atteintes à la vie privée sont frappées d'interdictions pénales d'une portée plus générale. En France, plusieurs de ces dispositions pénales sont spécifiquement conçues pour réprimer les activités de type « paparazzi », y compris l'utilisation par les médias des photographies ainsi obtenues. Ainsi, l'article 226-1 du Code pénal sanctionne le fait de porter atteinte à la vie privée d'autrui, notamment « en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ».

Cette approche par secteur présente de grands avantages, dans la mesure où certaines catégories de documents privés nécessitent une solide protection, à défaut de laquelle d'autres infractions pénales ou des préjudices civils risquent d'être commis. L'information bancaire est sans doute l'exemple le plus évident. Toutefois, l'expérience de nombreux pays montre qu'il n'est pas nécessaire d'ériger l'atteinte à la vie privée en infraction pénale générale, et qu'une telle règle risque en particulier d'être utilisée pour brider la liberté d'expression.

En droit international, et dans le droit de nombreux pays, ces protections ne peuvent être levées que lorsque l'intérêt public le commande de manière impérieuse. Un exemple classique en est la nécessité de faire respecter la loi (la police est autorisée à surveiller les communications dans le cadre d'une enquête criminelle). La levée de ces protections devrait être subordonnée à des conditions à la fois de procédure et de fond. Sur le plan de la procédure, il faut en principe obtenir un mandat judiciaire, et sur le fond faire la preuve de l'existence d'un intérêt public clair et primordial, comme la nécessité de faire la lumière sur une grave infraction pénale.

5.1.4 Les systèmes de protection des données

- Les États devraient mettre en place de solides régimes de protection des données comprenant les principaux éléments énumérés ci-dessous, à savoir un champ d'application étendu, le droit de donner ou non son consentement (droit d'opposition), le droit d'accès et de rectification, des obligations imposées aux responsables du traitement des données et le droit à réparation.
- Il convient de prévoir des exceptions à ces règles pour certains types de collecte de données, en particulier pour préserver le droit à la liberté d'expression.
- À défaut, les conflits entre le droit à la liberté d'expression, y compris le droit à l'information et les règles en matière de protection des données devraient être résolus conformément aux dispositions de la constitution en la matière, à savoir par des décisions dans lesquelles l'intérêt général prime sur le droit à la vie privée. Les réparations devraient aussi être proportionnées à la gravité des faits.

---

343 Un bon exemple en est la Loi sur la protection de la vie privée des conducteurs de véhicules adoptée aux États-Unis en 1994 (18 USC Chapter 123) pour faire face à la tendance croissante à vendre les informations personnelles sensibles figurant dans les dossiers d'enregistrement des véhicules motorisés.

On s'accorde aujourd'hui pour reconnaître que les régimes de protection des données sont une pièce essentielle de la protection plus générale de la vie privée, et certains de leurs éléments sont imposés par le droit international relatif aux droits de l'homme, de sorte qu'ils sont mis en place dans un nombre croissant de démocraties. Leurs principales caractéristiques sont décrites dans l'encadré XVI[344]. Un régime solide a pour éléments essentiels :

(1) **Un champ d'application étendu –** Les règles doivent s'appliquer aux ensembles de données personnelles et aux responsables du traitement des données du secteur public comme du secteur privé.

(2) **Le droit d'opposition –** Les intéressés doivent normalement être libres de consentir à la collecte de l'information ou de s'y opposer. Il ne devrait y avoir d'exception à cette règle que lorsque la collecte répond à un intérêt supérieur, défini par la loi. Cela implique que les intéressés comprennent les pratiques de l'organisme public ou privé qui collecte l'information et en aient été clairement informés au préalable. Une telle notification doit indiquer quelle est la nature de l'information qu'il est proposé de collecter et de conserver, qui sont les agents qui la collecteront, comment elle sera utilisée et qui y aura accès. Il doit être en outre clairement indiqué aux intéressés s'ils sont libres de fournir ou non l'information demandée ou si la loi leur en fait obligation, et quelles conséquences aurait dans ce cas le refus de fournir l'information. L'information ne doit pas être utilisée à des fins incompatibles avec l'usage à laquelle elle était destinée lors de sa collecte initiale.

(3) **Le droit à accès et à rectification –** Les intéressés doivent avoir le droit d'accéder à toute information les concernant à intervalles raisonnables et sans délais injustifiés. Ils doivent avoir aussi le droit de demander à l'organe responsable du traitement des données de rectifier toute erreur ou d'effacer les données, le cas échéant.

(4) **Des responsabilités imposées aux détenteurs de l'information –** Les responsables du traitement des données doivent prendre des mesures raisonnables pour s'assurer de l'exactitude et de la sécurité des données détenues par eux. L'accès aux données doit être limité conformément aux usages établis de ces données. Les données ne doivent être transmises à des tiers que si ceux-ci sont en mesure d'assurer un même respect des principes de protection des données. Sitôt qu'elles ne sont plus nécessaires pour les usages établis, les données doivent être détruites, ou converties en données anonymes. Tout au long de la période pendant laquelle les données sont conservées, des mesures doivent être prises pour en garantir la confidentialité, l'intégrité et la qualité.

(5) **Le droit de recours –** Les intéressés doivent disposer d'un droit de recours contre tout organisme public ou privé qui enfreint les règles de protection des données à l'égard des données les concernant. Des mesures correctrices peuvent être prises par voie d'autoréglementation, obtenues par des décisions de justice dans le cadre du droit privé, ou imposées par l'État. La surveillance du système doit être confiée à un organe indépendant.

---

344 Bien que décrivant le régime de protection des données institué par l'Union européenne, cet encadré reflète plus généralement les meilleures pratiques observées dans ce domaine.

Les régimes de protection des données plus aboutis prévoient des exceptions pour le traitement de données en rapport avec l'exercice du droit à la liberté d'expression (encore que le champ de ces exceptions soit parfois indûment restreint à l'utilisation des données à des fins journalistiques ou artistiques à l'exclusion des autres moyens d'expression, comme l'édition). Cela est important, en raison notamment du caractère très général des définitions de données personnelles utilisées dans ces régimes (données d'identification personnelle) et de l'absence de principes modulant l'utilisation des données (c'est-à-dire de systèmes donnant effet au primat de l'intérêt général).

Même lorsque les règles de protection des données sont d'application, les conflits entre droit à la vie privée et droit à la liberté d'expression doivent être résolus conformément aux dispositions générales en la matière telles qu'elles sont inscrites dans la constitution. En d'autres termes, il convient de déterminer ce que commande l'intérêt général.

Une question potentiellement plus complexe est celle de la relation entre le régime de protection des données et le régime d'accès à l'information. Dans ce domaine aussi, il est toutefois préférable de s'appuyer sur des protections et des définitions de la vie privée de portée générale, plutôt que d'inclure dans le régime de protection des données des règles spécialisées non conçues pour permettre un juste arbitrage entre l'accès et la confidentialité en matière de vie privée. Sachant que le droit à l'information est un aspect du droit à la liberté d'expression dans le droit international, cette approche est conforme à ce qui a été dit au point précédent (à savoir la mise en balance de la liberté d'expression et du droit à la vie privée). Elle est également en accord avec les principes fondamentaux du droit à l'information, y compris le fait que l'information doit être rendue publique lorsque l'intérêt général le commande, même si cela risque de porter atteinte à un intérêt protégé, comme le droit au respect de la vie privée.

5.2 Politiques et pratiques des sociétés commerciales

- Les sociétés commerciales devraient se doter d'une solide politique en matière de respect de la vie privée afin de protéger les utilisateurs. Cette politique devrait avoir pour principe général de permettre à ces derniers d'exercer le plus grand contrôle possible sur leur vie privée, et comporter des règles concernant toute modification ultérieure de la politique qui protègent les utilisateurs contre d'éventuels risques accrus d'intrusion dans leur vie privée. Une approche possible est décrite de manière plus détaillée ci-après.
- Il conviendrait de considérer avec plus d'attention des initiatives d'autoréglementation, voire de coréglementation, ainsi que les options fondées sur la coopération, comme moyens de protéger la vie privée des utilisateurs. Les sociétés commerciales devraient consacrer plus de temps et de ressources à cette importante question, en consultation avec les autres parties prenantes.
- Les sociétés commerciales devraient prendre l'engagement général d'accorder toute l'attention voulue aux questions se rapportant à la vie privée et à la liberté d'expression. La manière dont cet engagement se traduira dans la pratique dépendra des activités propres à chacune d'elles, mais il doit impliquer au moins que la société consacrera une part de son temps et de son énergie à réfléchir aux moyens d'adapter son activité de façon à mieux respecter ces droits fondamentaux. Dans la plupart des cas, il sera nécessaire d'élaborer la politique dans le cadre d'un processus transparent.

Comme on l'a déjà noté ailleurs dans ce rapport, les initiatives d'autoréglementation des sociétés commerciales ne vont pas de soi en matière de vie privée parce que, pour la plupart des fournisseurs d'accès à l'Internet et des fournisseurs de services en ligne, les intérêts commerciaux poussent tous dans le sens contraire, à l'exception du poids de l'opinion publique, qui ne représente un frein puissant que pour un nombre restreint d'entreprises. C'est pourquoi de nombreux commentateurs se montrent sceptiques à l'égard des efforts d'autoréglementation[345].

Dans le même temps, les bonnes pratiques commerciales sont un facteur essentiel de protection efficace de la vie privée en ligne. Sans doute la question la plus sensible est-elle celle du consentement, lequel, une fois donné, lève les principales règles de protection des données. C'est souvent par des mécanismes d'enregistrement des options que les utilisateurs consentent aux politiques et aux approches (souvent moins transparentes) des fournisseurs d'accès et de services en ligne. Nous l'avons vu, le bon fonctionnement de tels systèmes ne va pas sans soulever diverses difficultés, notamment la complexité (probablement nécessaire) de ces politiques et approches, le grand nombre de services différents utilisés et la faible mobilisation des utilisateurs sur cette question. À cela s'ajoute le fait que certaines sociétés modifient leurs règles de confidentialité. Tout cela a pour effet de transférer aux sociétés une bonne part des leviers de contrôle, et donc aussi des responsabilités.

Il est possible de recenser un certain nombre de bonnes pratiques dans ce domaine. En premier lieu, les sociétés commerciales devraient s'engager à adopter une politique transparente en matière de respect de la vie privée, généralement sur la base des normes décrites dans le présent rapport. Beaucoup de fournisseurs d'accès et de fournisseurs de services en ligne ne l'ont pas encore fait. Ces politiques doivent répondre aux besoins des consommateurs, et être par exemple facilement consultables sur le site Web du prestataire et rédigées, dans toute la mesure du possible, en des termes simples et intelligibles, dans une ou plusieurs langues.

Deuxièmement, le contrôle des données privées doit, chaque fois que possible – et notamment lorsque cela est compatible avec le service fourni et le modèle d'affaires de la société – être laissé à utilisateur. C'est ainsi que Facebook permet à ses utilisateurs de définir certains paramètres de confidentialité, au moins pour ce qui concerne les données auxquelles ont accès les autres utilisateurs, tandis que la politique de confidentialité de Google permet d'ajouter ou de retrancher diverses options[346]. Dans la mesure où l'ajout de nouvelles options demande une plus grande attention de la part de l'utilisateur, ce mécanisme apparaît préférable sur le plan de la protection de la vie privée.

Troisièmement, les sociétés devraient prendre certains engagements vis-à-vis des utilisateurs concernant les futurs changements apportés à leur politique de confidentialité. Google promet de ne pas restreindre la protection de la vie privée de ses utilisateurs sans leur consentement exprès. Facebook promet de laisser à ses utilisateurs un délai de 7 jours pour donner leur avis sur la plupart des changements éventuels, et si plus de 7 000 personnes postent des commentaires, ce qui n'est pas nécessairement une condition irréalisable compte tenu du très grand nombre total d'utilisateurs, de soumettre

---

345 Certaines de ces critiques ont été mentionnées plus haut. Voir la note 298 et le texte auquel elle se rapporte.

346 Cette politique peut être consultée à l'adresse suivante : http://www.google.com/policies/privacy/.

le changement envisagé à un vote. Quelle que soit l'issue de ce vote, la société s'y conformera à condition que 30 % au moins de tous les utilisateurs enregistrés y aient participé[347]. Ce seuil est très élevé (voir les faibles taux de participation, même à des scrutins nationaux, dans la plupart des pays), mais peut être pas impossible à atteindre en cas de changement très controversé.

À certains égards, le débat sur la politique des sociétés commerciales dans ce domaine ne fait que commencer. Il reste encore beaucoup à faire pour approfondir les idées, les tester et tenter de dégager un accord sur certaines pratiques optimales. Pour remédier aux insuffisances des politiques d'autoréglementation et des programmes lancés à l'instigation des sociétés commerciales, certains commentateurs ont appelé à des initiatives de coréglementation associant entreprises commerciales, organisations de la société civile et pouvoirs publics. Une réflexion plus poussée sera nécessaire pour déterminer si telles ou telles propositions sont ou non réalisables ou si elles présentent plus de risques que d'avantages pour les intérêts mêmes qu'elles sont censées défendre, à savoir le respect de la vie privée et la liberté d'expression.

L'idée d'arrangements de coopération pourrait elle aussi se révéler fructueuse. La coopération diffère de la coréglementation de par son caractère librement consenti, tout en ayant en commun avec elle le fait d'associer les acteurs publics et les acteurs privés. La certification officielle des fournisseurs de services apparaît comme une piste prometteuse. Elle suppose un accord sur un ensemble de normes fondamentales, puis la certification des sociétés appliquant ces normes. Différentes options pourraient être explorées concernant le contrôle du système, qui pourrait être confié à un organisme public indépendant, comme l'autorité de régulation des télécommunications existant dans de nombreux pays, ou à un organisme du secteur d'activité, le respect des règles étant assuré par divers arrangements de coopération.

Même s'il faut encore réfléchir plus avant à ces questions, certaines sociétés tentent d'ores et déjà d'élaborer de meilleures options pour protéger la vie privée en ligne. Un exemple en est la société Mozilla, qui fournit le navigateur Firefox[348]. Une politique de confidentialité s'inspirant de l'approche de cette société pourrait reposer sur les principes suivants :

(1) **Pas de surprises.** L'entreprise ou le prestataire de services n'utilise, collecte et partage l'information relative aux utilisateurs que conformément à des règles publiées dans un langage clair, concis et facile à comprendre.

(2) **Des choix réels.** La société ou le prestataire de services offre aux utilisateurs la possibilité de faire des choix concrets et éclairés en l'informant clairement au stade de la collecte et en lui laissant la liberté de revenir sur ses choix chaque fois que possible.

(3) **Des paramètres raisonnables.** La société ou le prestataire de services établit pour ses produits ou services des paramètres par défaut représentant le meilleur équilibre entre la protection de la vie privée, la sécurité et le degré d'expérience de l'utilisateur.

(4) **Une collecte limitée des données.** La société ou le prestataire de services ne collecte et conserve que la quantité de données strictement nécessaire à l'utilisation du produit ou du service et répond aux attentes raisonnables de l'utilisateur en

347 Cette politique peut être consultée à l'adresse suivante : http://www.facebook.com/about/privacy/.
348 http://www.mozilla.org/about/policies/privacy-policy.html .

matière de confidentialité. Il utilise des agrégats anonymes de données chaque fois que possible, et ne conserve les informations personnelles qu'aussi longtemps que cela est nécessaire pour les fins auxquelles elles ont été collectées.

(5) **Contrôle exercé par l'utilisateur.** La société ou le prestataire de services ne capte ni ne divulgue aucune information personnelle relative à l'utilisateur sans le consentement de celui-ci. Il utilise des dispositifs de renforcement de la confidentialité qui permettent à l'utilisateur de garder le contrôle de l'information le concernant et lui permettent de savoir comment cette information est utilisée et de mettre fin à sa collecte et à son captage lorsqu'il le souhaite.

(6) **Accès de l'utilisateur.** L'utilisateur a le droit de savoir quand des données le concernant sont collectées ou traitées et d'y avoir accès sous une forme intelligible. Cet accès doit lui être fourni sans frais, et il doit lui être possible d'effacer l'information ou de la corriger si elle est erronée.

(7) **Fiabilité des partenaires.** La société ou le prestataire de services doit faire de la protection de la vie privée un critère essentiel du choix de ses partenaires et de ses relations avec eux. De plus, les sociétés, prestataires de services et fournisseurs d'applications avec lesquels il entretient de telles relations doivent respecter les mêmes principes en matière de confidentialité.

(8) **Sécurité.** La société ou le prestataire de services doit prendre toute mesure appropriée pour protéger les données contre les risques naturels et humains, y compris l'accès non autorisé, l'utilisation abusive ou l'erreur. En cas de défaillance de la sécurité d'un site Web ou d'un service, l'utilisateur a le droit d'en être immédiatement informé.

(9) **Transparence de la communication de données aux pouvoirs publics.** La société ou le prestataire de services doit notifier à l'utilisateur les demandes d'information concernant ses comptes faites par les pouvoirs publics, lorsque la loi l'y autorise, de manière que l'utilisateur ait la possibilité, s'il le souhaite, de s'opposer à cette demande.

(10) **Réparations.** Lorsque la société constate qu'elle a porté atteinte ou contribué à porter atteinte à la vie privée de l'utilisateur, elle doit prendre des dispositions pour enregistrer sa plainte ou contribuer à son enregistrement et offrir des réparations à l'utilisateur à l'issue d'un processus transparent.

(11) **Protection généralisée de la vie privée.** Les protections de la vie privée doivent s'appliquer de manière uniforme à toutes les plates-formes en ligne et mobiles et à l'ensemble des sociétés, prestataires de services et fournisseurs d'applications tiers. La société doit également s'assurer que ses partenaires appliquent des principes stricts en matière de confidentialité.

Les éventuels conflits avec le droit à la liberté d'expression soulèvent des difficultés pour les fournisseurs d'accès à l'Internet et les fournisseurs de services en ligne. Les sociétés qui opèrent dans les nombreux pays où le cadre juridique n'assure pas une solide protection du droit à la liberté d'expression sont souvent confrontées à des choix épineux, comme en témoignent les problèmes mentionnés plus haut de Yahoo! en

Chine. Pour se soustraire à de tels dilemmes, Google a mis fin à ses activités en Chine continentale en mars 2010[349].

Dans beaucoup d'autres pays, les sociétés disposent d'un certain nombre d'options, depuis les approches les plus « dures », consistant par exemple à invoquer la législation pour faire reconnaître leurs droits face à des gouvernements qui tentent de limiter la protection de la vie privée et/ou la liberté d'expression, jusqu'à des méthodes plus souples, mais souvent très efficaces, tendant à utiliser leurs moyens (considérables dans le cas des grandes sociétés internationales) pour sensibiliser à ces droits le personnel et les membres des organes de gouvernance, à partager l'information concernant les problèmes et les solutions, à analyser les risques et à concevoir des réponses et des solutions, et à évaluer régulièrement les progrès accomplis. Bon nombre de ces stratégies sont décrites en détail dans les Directives de mise en œuvre publiées par l'Initiative mondiale des réseaux (GNI)[350]. Beaucoup nécessitent une volonté politique, qui semble malheureusement faire défaut à bon nombre de fournisseurs d'accès et de services, témoin le fait que cinq sociétés commerciales seulement sont membres du GNI.

5.3 Sensibilisation du public

- Les États devraient entreprendre de sensibiliser le public aux problèmes de la protection de la vie privée à l'ère des nouvelles technologies, en s'adressant aux jeunes par l'intermédiaire du système éducatif, et en utilisant d'autres structures pour toucher les adultes.
- D'autres acteurs à même de sensibiliser l'opinion – comme les sociétés commerciales, les parents et les groupes de la société civile – devraient également contribuer à une meilleure compréhension de la protection de la vie privée à l'ère des nouvelles technologies.
- Les médias ont un grand rôle à jouer en faisant prendre conscience de l'importance de la protection de la vie privée et des différents obstacles qui surgissent à mesure du développement de l'Internet. Le récent scandale qui a conduit un journal à fort tirage du Royaume-Uni accusé d'avoir piraté le téléphone mobile de victimes de criminels à mettre fin à sa publication montre à quel point la méconnaissance de la nécessité de respecter la vie privée en ligne peut nuire à la réputation des médias. Les journalistes doivent être conscients, et faire prendre conscience, des incidences des nouvelles technologies pour les médias et des risques de violation de la vie privée. Dans le même temps, les médias doivent être attentifs au fait que les contrôles exercés au nom du respect de la vie privée ne sont pas toujours assortis de garde-fous suffisants pour protéger la liberté d'expression.

Aucun ensemble de recommandations pratiques concernant la vie privée et la liberté d'expression sur l'Internet ne saurait être complet s'il passe sous silence les principaux utilisateurs de l'Internet, c'est-à-dire le grand public. Les utilisateurs peuvent faire eux-mêmes beaucoup pour protéger leur propre vie privée et leur propre liberté d'expression en

---

349 Voir l'annonce publiée par Google à ce sujet à l'adresse suivante : http://googleblog.blogspot.ca/2010/03/new-approach-to-china-update.html.

350 Disponible à l'adresse suivante : http://globalnetworkinitiative.org/implementationguidelines/index.php.

ligne. Même des dispositifs relativement sophistiqués comme les outils de cryptage sont aujourd'hui à la portée de tout un chacun et, sans aller chercher aussi loin, la connaissance de certaines réalités simples concernant les nouvelles technologies, comme le fait que des employeurs utilisent l'Internet pour se renseigner sur les antécédents des candidats à un poste peut inciter à plus de prudence au moment de définir les paramètres de confidentialité sur Facebook.

L'initiation aux médias et à l'Internet devrait faire partie, dès le tout jeune âge, de l'enseignement des compétences de la vie courante dispensé par le système éducatif, dans le cadre plus général des cours d'éducation civique ou de développement personnel. Les États devraient également faire des efforts pour familiariser les adultes avec la problématique de la protection de la vie privée à l'ère des nouvelles technologies, par exemple en élaborant des matériels de sensibilisation et en les mettant à la disposition du public en ligne et dans des lieux appropriés.

De nombreux autres acteurs sociaux peuvent également jouer un rôle dans ce domaine. Les fournisseurs d'accès et les fournisseurs de services en ligne devraient s'efforcer d'appeler l'attention des utilisateurs sur les risques liés aux « négligences » à l'égard de la protection de leur vie privée, sachant qu'il peut être difficile d'obtenir d'une société commerciale qu'elle mette en garde des clients potentiels contre les risques que présente l'utilisation de ses propres services. Les médias devraient traiter de cette question dans le cadre général de leur mission d'information du public sur les questions d'intérêt général. De nombreuses organisations de la société civile travaillent dans des domaines où la protection de la vie privée est un aspect important ou pertinent, et devraient elles aussi inclure des campagnes de sensibilisation au nombre de leurs activités. Les parents devraient être eux aussi encouragés à protéger leurs enfants en les mettant en garde contre les risques de violation de la vie privée sur l'Internet. La tâche est immense, mais les efforts concertés de l'ensemble des acteurs concernés peuvent beaucoup.

6. RESSOURCES UTILES

On trouvera ci-après une compilation d'informations concernant le respect de la vie privée et la liberté d'expression sur l'Internet qui ont été réunies par nos soins. Cette masse d'information est organisée de manière à couvrir les cinq régions suivantes : Afrique, Asie et Pacifique, Amérique latine et Caraïbes, États arabes, et Europe et Amérique du Nord. Une dernière section est plus spécialement consacrée aux questions relatives au genre. Les documents, rapports, ouvrages et articles ainsi compilés ont été obtenus auprès de bibliothèques de recherche ainsi que d'organisations non gouvernementales et de centres universitaires de premier plan travaillant sur ces questions. Dans chacune des sections – documentation générale et régions – un certain nombre de documents considérés comme présentant un intérêt tout particulier sont cités en premiers. Nos recherches ont pris fin le 6 juillet. À cette date, tous les liens indiqués ci-après étaient actifs.

6.1 Documentation générale

Banisar, D. et Davies, D. (1999), « Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments », disponible à l'adresse suivante : http://www.jcil.org/journal/articles/117.html

Faris, R., Wang, S. et Palfrey, J. (2008), « Censorship 2.0 » Innovations: Technology|Governance|Globalization, disponible à l'adresse suivante : http://www.mitpressjournals.org/doi/abs/10.1162/itgg.2008.3.2.165

Lanois, P. (2011), « Privacy in the age of the cloud », Journal of Internet Law, ISSN 1094-2904, 12/2011, Volume 15, Issue 6, p. 3.

Bambauer, D., Palfrey, J., et Zittrain, J. (2004), « A Starting Point: Legal Implications of Internet Filtering », Open Net Initiative, disponible à l'adresse suivante : http://opennet.net/docs/Legal_Implications.pdf

Boyd, D. (2010). « Living Life in Public: Why American Teens Choose Publicity Over Privacy. » Association of Internet Researchers. Göteborg (Suède), disponible à l'adresse suivante : http://www.danah.org/papers/talks/2010/AOIR2010.html

Boyd, D. (2010). « Making Sense of Privacy and Publicity. » SXSW. Austin, TX., disponible à l'adresse suivante : http://www.danah.org/papers/talks/2010/SXSW2010.html

Boyd, D. (2010). « Privacy and Publicity in the Context of Big Data. » Raleigh, NC, disponible à l'adresse suivante : http://www.google.com.ar/url?sa=t&rct=j&q=%22privacy%20and%20publicity%20in%20the%20context%20of%20big%20data&source=Web&cd=1&ved=0CGAQFjAA&url=http%3A%2F%2Fwww.danah.org%2Fpapers%2Ftalks%2F2010%2FWWW2010.html&ei=cTD3T_fSE4OE8ASPw8TuBg&usg=AFQjCNHvgZNDYr_f3a28tOWhUIHFyHdq4A

Boyd, D. (2010). « Privacy, Publicity, and Visibility. » Microsoft Research TechFest. Redmond, WA.

Boyd, D. (2010), « The Future of Privacy: How Privacy Norms Can Inform Regulation ». Conférence internationale des commissaires à la protection des données et de la vie privée. Jérusalem (Israël), disponible à l'adresse suivante : http://www.danah.org/papers/talks/2010/PrivacyGenerations.html

Boyd, D. (2011), « Networked Privacy ». Personal Democracy Forum. New York, NY, 6 juin, disponible à l'adresse suivante : http://www.danah.org/papers/talks/2011/PDF2011.html

Boyd, D. et Marwick, A. (2011). « Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. » Document présenté à l'Oxford Internet Institute dans le cadre du colloque “A Decade in Internet Time”, 22 septembre, disponible à l'adresse suivante : http://www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf

Boyd, D. et Marwick, A. (2011). « Social Steganography: Privacy in Networked Publics. » International Communication Association. Boston, MA, disponible à l'adresse suivante : http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf

Brunton, F., et Nissenbaum, H. (2011), « Vernacular resistance to data collection and analysis: A political theory of obfuscation », First Monday, Volume 16, Number 5, disponible à l'adresse suivante : http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955

Deibert, R. (2000), « International Plug n' Play? Citizen Activism, the Internet, and Global Public Policy, » International Studies Perspectives, Vol. 1, n° 3, pp. 255-272.

Deibert, R. (2003), « Black Code: Censorship, Surveillance, and Militarization of Cyberspace, » Millennium: Journal of International Studies, Vol. 32, n°. 3.

Deibert, R. (2004), « Firewalls and Power: An Overview of Global State Censorship of the Internet », avec Nart Villeneuve, in Klang, M. & Murray, A. (dir. publ.) Human Rights in the Digital Age, Cavendish Publishing London.

EFF (2011), « Freedom of Expression, Privacy and Anonymity on the Internet. Comments submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression », disponible à l'adresse suivante : https://www.eff.org/sites/default/files/filenode/UNSpecialRapporteurFOE2011-final_3_0.pdf

Faris, R. et Zittrain, J. (2009), « Web tactics » Index on Censorship, 38 ; 90, disponible à l'adresse suivante : http://ioc.sagepub.com/content/38/4/90.full.pdf+html

Franda, M. (2002), Internet and the Cyberspace, Internet Development and Politics in Five World Regions, Lynne Rienner Publishers, inc., États-Unis d'Amérique et Royaume-Uni, disponible à l'adresse suivante : http://books.google.com.ar/books?hl=es&lr=&id=k89jJKN1wXcC&oi=fnd&pg=PR11&dq=privacy+and+Internet+arab+region&ots=aYTBncvUIw&sig=4vOeAgHxO5UWDquGdba1EE18Kks#v=onepage&q=privacy%20and%20internet%20arab%20region&f=false

Global Network Initiative (2010), Inaugural Report 2010. Our work. Our vision. Our progress, disponible à l'adresse suivante : http://www.globalnetworkinitiative.org/files/GNI_Annual_Report_2010.pdf

Hartzog, W. (2009), « The privacy box: A software proposal », First Monday, Volume 14, Number 11-2, disponible à l'adresse suivante : http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2682/2361

Forum sur la gouvernance de l'Internet (2010), Developing the Future Together, publié par Brian Gutterman, Cinquième réunion du Forum sur la gouvernance de l'Internet, Vilnius (Lituanie), disponible à l'adresse suivante : http://www.intgovforum.org/cms/2011/book/IGF_2010_Book.pdf

Leon, P., Ur, B., Balebako, R., Cranor, L., Shay, R. et Wa, Y (2011), « Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising », disponible à l'adresse suivante : http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html

Madrid Privacy Declaration (2011), disponible à l'adresse suivante : http://thepublicvoice.org/madrid-declaration/fr/

Marwick, A., Murgia Diaz, D., et Palfrey, J. (2010), « Youth, Privacy and Reputation », disponible à l'adresse suivante : http://cyber.law.harvard.edu/publications/2010/Youth_Privacy_Reputation_Lit_Review

Palfrey, J. (2008), « The Public and the Private at the United States Border with Cyberspace », disponible à l'adresse suivante : http://cyber.law.harvard.edu/publications/2008/Public_and_Private_at_US_Border_with_Cyberspace

Palfrey, J. et Rogoyski, R. (2006), « The Move to the Middle: The Enduring Threat of 'Harmful' Speech to Network Neutrality, » Washington University Journal of Law and Policy.

Privacy International (2012), An assessment of the EU-US travel surveillance agreement, disponible à l'adresse suivante : https://www.privacyinternational.org/reports/an-assessment-of-the-eu-us-travel-surveillance-agreement

Raynes-Goldie, K. (2010), « Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook », First Monday, Volume 15, Number 1-4, disponible à l'adresse suivante : http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Rodriguez, K (2012), « Biometric National IDs and Passports: A False Sense of Security », disponible à l'adresse suivante : https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security

Assemblée générale des Nations Unies (2012), « La promotion, la protection et l'exercice des droits de l'homme sur l'Internet », disponible à l'adresse suivante : http://www.unaf.fr/IMG/pdf/g1214711.pdf

Van den Berg, B. et Van der Hof, S. (2012), « What happens to my data? A novel approach to informing users of data processing practices », First Monday, Volume 17, Number 7, disponible à l'adresse suivante : http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/4010/3274 .

Van Schewick, B. (2012), « Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like », disponible à l'adresse suivante : http://cyberlaw.stanford.edu/publications

Villeneuve, N. (2006), «The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace» First Monday, Volume 11, disponible à l'adresse suivante : http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227

Volokh, E. (1999), « Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You », disponible à l'adresse suivante : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469

Zittrain, J. (2003), « Internet Points of Control », Boston College Law Review, disponible à l'adresse suivante : http://cyber.law.harvard.edu/publications/2003/Internet_Points_of_Control

Zittrain, J. (2003), « Be Careful What You Ask For: Reconciling a Global Internet and Local Law » (PDF), Who Rules the Net? The Cato Institute, disponible à l'adresse suivante : http://cyber.law.harvard.edu/node/367

Zittrain, J. (2006), «The Generative Internet», Harvard Law Review, Vol. 119, p. 1974, mai 2006, disponible à l'adresse suivante : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=847124

6.2 Afrique

Thabang Masete, N, (2012), « The Challenges in Safeguarding Financial Privacy in South Africa », Journal of International Commercial Law and Technology, ISSN 1901-8401, 07/2012, Volume 7, Issue 3, p. 248-259

Olinger, H., Britz, J. et Olivier, M. (2007), « Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa », International Information and Library Review, ISSN 1057-2317, 2007, Volume 39, Issue 1, p. 31-43

Mivule, K. et Turner, C. (2011), « Applying Data Privacy Techniques on Tabular Data in Uganda », disponible à l'adresse suivante : http://arxiv.org/abs/1107.3784

Open Net Initiative (2009), « Internet Filtering in Sub-Saharan Africa », disponible à l'adresse suivante : http://opennet.net/sites/opennet.net/files/ONI_SSAfrica_2009.pdf

Ncube, C. (2004), « A Comparative Analysis of Zimbabwean and South African Data Protection Systems », Journal of Information, Law and Technology, disponible à l'adresse suivante : http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/caroline.doc

Banisar, D. (2009), « ICT policies relating to privacy, freedom of expression and access to information : a briefing paper », Université Makerere, Human Rights and Peace Centre, disponible à l'adresse suivante : http://idl-bnc.idrc.ca/dspace/handle/10625/41470

Boniface Makulilo, A. (2012), Privacy and data protection in Africa: a state of the art, Oxford University Press, disponible à l'adresse suivante : http://idpl.oxfordjournals.org/content/early/2012/06/11/idpl.ips014.full

Cohen, T. (2000), « But for the nicety of knocking and requesting a right of entry': surveillance law and privacy rights in South Africa », disponible à l'adresse suivante : http://idl-bnc.idrc.ca/dspace/handle/10625/42079

Faris, R., Roberts, H., Heacock, R., Zuckerman, E. et Gasser, E. (200x), « Online Security in the Middle East and North Africa. A Survey of Perceptions, Knowledge, and Practice », Harvard Cyber Law, disponible à l'adresse suivante : http://cyber.law.harvard.edu/node/6973

CRDI, « Protection de la vie privée des jeunes en Amérique latine », disponible à l'adresse suivante : http://www.idrc.ca/FR/Programs/Science_and_Innovation/Information_and_Networks/Pages/ResultDetails.aspx?ResultID=54

Kofi-Armah, D., (2012), Internet Security and Data Protection in Ghana, Africa: A Hacker's Perspective, disponible à l'adresse suivante : http://www.connectedafrica.com/internet-security-and-data-protection-in-ghana-africa-a-hackers-perspective-interview-with-sepo/

MacKinon, R., Risen, T., Hussain, H., Li, W., Losey, J. et Myers, S. (2012), Le Netizen Report : Édition Transition, Global Voices Online, publié le 14 juin 2012, disponible à l'adresse suivante : http://fr.globalvoicesonline.org/2012/07/03/113862/

Makulilo, A. (2012), « Privacy and data protection in Africa: a state of the art », International Data Privacy Law, disponible à l'adresse suivante : http://idpl.oxfordjournals.org/content/early/2012/06/11/idpl.ips014.abstract

Privacy International (2006), Afrique du Sud, disponible à l'adresse suivante : https://www.privacyinternational.org/reports/south-africa

6.3 États arabes

Aladwani, A.M. (2003), Key Internet characteristics and e-commerce issues in Arab countries, information Technology & People, Vol. 16 Iss: 1, p. 9-20, disponible à l'adresse suivante : http://www.emeraldinsight.com/journals.htm?articleid=883574&show=abstract

Warf, B. et Vincent, P. (2007), Multiple geographies of the Arab Internet, Area Volume 39, Issue 1, p. 83-96, mars 2007, disponible à l'adresse suivante : http://onlinelibrary.wiley.com/doi/10.1111/j.1475-4762.2007.00717.x/full

Al-Rasheed, A. (2001), « The Internet in Saudi Arabia », disponible à l'adresse suivante : http://www.isu.net.sa/library/CETEM2001-AlRasheed.pdf

Bureau of Democracy (2007), Human Rights, and Labor, Iraq, Département d'État des États-Unis.

Burkhart, E. (1998), « National Security and the Internet in the Persian Gulf Region », disponible à l'adresse suivante : http://www.georgetown.edu/research/arabtech/pgi98-10.html

Messieh, N. (2011), « Discover Digital Arabia: Middle East Internet usage in numbers », disponible à l'adresse suivante : http://thenextWeb.com/me/2011/08/25/discover-digital-arabia-middle-east-Internet-usage-in-numbers/

Noman, H. (2009), « An Overview of The Demographics and Usage Patterns of Internet Users in Developing Countries: Yemeni Internet Population as a Case Study », Programme des Nations Unies pour le développement, disponible à l'adresse suivante : http://opennet.net/sites/opennet.net/files/ONI_Yemen_2009.pdf

Open Net Initiative (2004), « Internet Filtering in Saudi Arabia », disponible à l'adresse suivante : http://opennet.net/studies/saudi

Open Net Initiative (2005), « Internet Filtering in Bahrain in 2004-2005 », disponible à l'adresse suivante : http://opennet.net/studies/bahrain

Open Net Initiative (2005), « Internet Filtering in Iran in 2004-2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/iran

Open Net Initiative (2005), « Internet Filtering in the United Arab Emirates in 2004-2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/uae

Open Net Initiative (2005), « Internet Filtering in Yemen in 2004-2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/yemen

OpenNet Initiative (2004), Internet Filtering in Saudi Arabia, disponible à l'adresse suivante : http://www.opennetinitiative.net/studies/saudi/#toc4c

Privacy International (2006), United Arab Emirates, disponible à l'adresse suivante : https://www.privacyinternational.org/reports/united-arab-emirates

Privacy International (2006), Iraq, disponible à l'adresse suivante : https://www.privacyinternational.org/reports/united-arab-emirates

Rohozinski, R. (2004) « Secret Agents » and « Undercover Brothers »: The Hidden Information Revolution in the Arab World », disponible à l'adresse suivante : http://mediaresearchhub.ssrc.org/201csecret-agents201d-and-201cundercover-brothers201d-the-hidden-information-revolution-in-the-arab-world/attachment

Sait, S., Ali, S., Al-Tawil, K. et Sanaullah, S (2010), « Trends in Internet Usage & its Social Effects in Saudi Arabia », disponible à l'adresse suivante : http://www.google.com.ar/url?sa=t&rct=j&q=saudi%20arabia%20privacy%20internet&source=Web&cd=5&ved=0CGcQFjAE&url=http%3A%2F%2Ffaculty.kfupm.edu.sa%2Fcoe%2Fsadiq%2Frichfiles%2Frich%2Fdoc%2FSocialEffectsTrends.doc&ei=-CL3T_-yM4aQ8wSi0KSJBw&usg=AFQjCNGL6f6FgAK5e1hDNLiEaXff8QcwpA

Zittrain & Edelman, « Documentation of Internet Filtering in Saudi Arabia », disponible à l'adresse suivante : http://cyber.law.harvard.edu/filtering/saudiarabia/sa-yahoo-3.html

6.4 Asie et Pacifique

Open Net Initiative (2009), « Internet Filtering in Asia », disponible à l'adresse suivante : http://opennet.net/sites/opennet.net/files/ONI_Asia_2009.pdf

Chung, R. (2003), Hong Kong's « Smart » Identity Card: Data Privacy Issues and Implications for a Post-September 11th America, Asian-Pacific Law & Policy Journal ; Vol. 4, Issue 2

Jho, W. (2005), « Challenges for e-governance: protests from civil society on the protection of privacy in e-government in Korea », disponible à l'adresse suivante : http://ras.sagepub.com/content/71/1/151.abstract

Gomez, J. (2003), « Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia », Pacific Journalism Review, disponible à l'adresse suivante : http://gomezcentre.academia.edu/JamesGomez/Papers/116683/Dumbing_down_democracy_trends_in_internet_regulation_surveillance_and_control_in_Asia

Kitiyadisai, K., (2005), « Privacy Rights and Protection: Foreign Values in Modern Thai Context », Ethics and Information Technology », disponible à l'adresse suivante : http://www.stc.arts.chula.ac.th/feeds/Krisana/7156321v361p0324.pdf

Chik, W. (2006), « The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore – Two Differing Asian Approaches », International Journal of Law and Information Technology, ISSN 0967-0769, 04/2006, Volume 14, Issue 1, p. 47.

Greenleaf, G. (2012), « Promises and illusions of data protection in Indian law », disponible à l'adresse suivante : http://idpl.oxfordjournals.org/content/1/1/47.full.pdf+html

ARTICLE 19 (2011), »South East Asia: the state of free expression », disponible à l'adresse suivante : http://www.article19.org/resources.php/resource/2258/en/south-east-asia:-the-state-of-free-expression

Cheung, A., (2009), « China Internet going wild: Cyber-hunting versus privacy protection », disponible à l'adresse suivante : http://www.sciencedirect.com/science/article/pii/S026736490900065X

Wu, Y., Lau, T., Atkin, D. et Lin, C., (2011), « A comparative study of online privacy regulations in the U.S. and China », Telecommunications Policy, ISSN 0308-5961, 2011, Volume 35, Issue 7, p. 603 – 616.

Viner, N., (2007), « The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century? », Iowa Law Review ; 11/1/2007, Vol. 93 Issue 1, p. 361-391.

Bamman, D., O'Connor, B. et Smith, N. (2011), « Censorship and deletion practices in Chinese social media », First Monday, Volume 17, Number 3, disponible à l'adresse suivante : http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3943/3169

Deibert, R. (2001), «Dark Guests and Great Firewalls: Chinese Internet Security Policy », Journal of Social Issues, 58, 1: 143-158.

Deibert, R. (2006), « The geopolitics Asian Cyberspace », Far Eastern Economic Review, disponible à l'adresse suivante : http://www.feer.com/articles1/2006/0612/free/p022.html

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (2011), « Access Contested: Security, Identity, and Resistance in Asian Cyberspace », Harvard Cyber Law, disponible à l'adresse suivante : http://oni-access.net/contested/

Greenleaf , G (2011), 'Outsourcing and India's new privacy law: No cause for panic, Privacy Laws & Business International Report, Issue 111, 16-17, avril 2011

Greenleaf, G (2011c), 'Breach notification and diffused enforcement in Taiwan's DP Act' Privacy Laws & Business International Report, Issue 109, 12-13, février, 2011

Greenleaf, G (2011a), « India attempts data protection by regulations », Privacy Laws & Business International Report, Issue 110, avril 2011.

Open Net Initiative (2005), « Internet Filtering in Burma in 2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/burma

Open Net Initiative (2005), « Internet Filtering in China in 2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/china

Open Net Initiative (2005), « Internet Filtering in Singapore in 2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/singapore

Open Net Initiative (2005), « Internet Filtering in Tunisia in 2005: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/tunisia

Open Net Initiative (2006), « Internet Filtering in Vietnam in 2005-2006: A Country Study », disponible à l'adresse suivante : http://opennet.net/studies/vietnam

Rohozinski, R. (1999), « Mapping Russian Cyberspace: Perspectives on Democracy and the Net» (PDF), UNRISD, Document de discussion n° 115.

Rohozinski, R. (2000), « How the Internet Did Not Transform Russia », Current History, Volume 99, n° 334.

6.5 Amérique latine et Caraïbes

Bertoni, E. (2012), « Towards an Internet Free of Censorship. Proposals for Latin America », Universidad de Palermo, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información, disponible à l'adresse suivante : http://www.palermo.edu/cele/english/publication.html

Remolina, N. (2010), « ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? », International Law, Revista Colombiana de Derecho Internacional, 16(2010), p. 493.

Leonardi, M. (2005), « Responsabilidade Civil dos Provedores de Serviços de Internet », Thèse de doctorat initialement publiée par Juarez de Oliveira, 2005, São Paulo.

Albornoz, B., Barindelli, F., Caballero, J., Duaso, R., et Esquivel, W. (2011), « Derechos y justicia y el movimiento social en Internet », Instituto de Investigación para la Justicia, AR, disponible à l'adresse suivante : http://hdl.handle.net/10625/46335

Barindelli, F. et Gregorio, C. (2010), « Datos personales y libertad de expresión en las redes sociales digitales : memorándum de Montevideo », Ad-Hoc, Buenos Aires, AR, disponible à l'adresse suivante : http://hdl.handle.net/10625/46022

Bossio Montes de Oca, J, (2009), « Peru : the battle for control of the internet », Association for Progressive Communications, Quito, EC, disponible à l'adresse suivante : http://hdl.handle.net/10625/42792

Carvalho Lima, C.C. & Leite Monteiro, R. (2011), Comentários ao Anteprojeto de Lei sobre Proteção de Dados Pessoais (Observations sur la nouvelle loi brésilienne relative à la protection des données), Observatório da Internet.br – observatório brasileiro de políticas digitais (Observatoire de l'Internet – Observatoire brésilien des politiques numériques), disponible à l'adresse suivante : http://securitybreaches.files.wordpress.com/2011/05/anteprojeto-de-lei-brasileiro-sobre-protecao-de-dados-pessoais.pdf

Gregorio, C. et Ornelas, L. (2011), « Protección de datos personales en las redes sociales digitales : en particular de niños y adolescentes; memorándum de Montevideo », Instituto de Investigación para la Justicia, Buenos Aires, disponible à l'adresse suivante : http://hdl.handle.net/10625/46963

Gregorio, C.G. (2004), « Protección de Datos Personales: Europa Vs. Estados Unidos, Todo un Dilema para América Latina », disponible à l'adresse suivante : http://www.bibliojuridica.org/libros/3/1407/12.pdf

Instituto de Investigación para la Justicia (2004), « Internet, privacidad y sistema judicial en América Latina y el Caribe », IIJ, Buenos Aires, AR, disponible à l'adresse suivante : http://idl-bnc.idrc.ca/dspace/handle/10625/25922

Monteiro, R et Laurant, C. (2011), « New Brazilian data protection bill adopts data breach notification regime », disponible à l'adresse suivante : http://blog.security-breaches.com/2011/05/09/new_brazilian_data_protection_bill_adopts_data_breach_notification_regime/

OEA (2010), « Principes et recommandations préliminaires relatifs à la protection des données », disponible à l'adresse suivante : http://scm.oas.org/IDMS/Redirectpage.aspx?class=CP/CAJP&classNum=2921&lang=f

Privacy International (2011), « Guía de privacidad para hispanohablantes », disponible à l'adresse suivante : https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes

Rodriguez, K., (2011), « The Politics of Surveillance: The Erosion of Privacy in Latin America », disponible à l'adresse suivante : http://advocacy.globalvoicesonline.org/2011/07/27/the-politics-of-surveillance-the-erosion-of-privacy-in-latin-america/

6.6 Europe et Amérique du Nord

Carter, E. (2005), « Outlaw Speech on the Internet: Examining the Link Between Unique Characteristics of Online Media and Criminal Libel Prosecutions », Santa Clara Computer and High Technology Law Journal 21. 2 (Jan 2005): 289-318, disponible à l'adresse suivante : http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1376&context=chtlj

Elwood, S. and Leszczynski, A. (2010), Privacy, reconsidered: New representations, data practices, and the geoWeb, University of Washington, disponible à l'adresse suivante : http://www.sciencedirect.com/science/article/pii/S001671851000093X

Lin, E. (2002), Prioritizing Privacy: A Constitutional Response to the Internet, Berkeley Technology Law Journal, disponible à l'adresse suivante : http://www.law.berkeley.edu/journals/btlj/articles/vol17/LIN.pdf

Burghardt, T., Böhm, K., Buchmann, E., Kühling, J. et Sivridis A. (2009), A Study on the Lack of Enforcement of Data Protection Acts, disponible à l'adresse suivante : http://dbis.ipd.uni-karlsruhe.de/download/bu09edemocracy.pdf

Kuan Hon, W., Millard, C. and Walden, I. (2011), « The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing », Oxford University Press, disponible à l'adresse suivante : http://idpl.oxfordjournals.org/content/1/4/211.full

Access Now.org, European Digital Rights, Transatlantic Consumer Dialogue (2012), ¿Qué hace que el ACTA sea tan controversial? (Y porque a los euro-parlamentarios debería importarles), disponible à l'adresse suivante : http://www.manzanamecanica.org/files/ACCESS_EDRI_TACD-por_que_oponerse_al_acta_ES.pdf

La Quadrature Du Net, Internet & Libertés (2012), Remporter une ÉNORME victoire contre l'ACTA et au-delà !, disponible à l'adresse suivante : http://www.laquadrature.net/fr/remporter-une-enorme-victoire-contre-lacta-et-au-dela

American Civil Liberties Union (2011), Government Requests For Twitter Users' Personal Information Raise Serious Constitutional Concerns, Says ACLU, disponible à l'adresse suivante : http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu

Budish, R. (2007), In the Face of Danger: Facial Recognition and the Limits of Privacy Law, disponible à l'adresse suivante : http://hlr.rubystudio.com/media/pdf/facial_recognition_privacy_law.pdf

Conseil de l'Union européenne (2011), Acuerdo Comercial de Lucha Contra la Falsificación (ACTA), disponible à l'adresse suivante : http://register.consilium.europa.eu/pdf/es/11/st12/st12196.es11.pdf, disponible en français à l'adresse suivante : http://register.consilium.europa.eu/pdf/fr/11/st12/st12196.fr11.pdf (Accord commercial anti contrefaçon).

De Gucht, K (2012), ACTA: « Making the right choice », Parlement européen, Commission du commerce international, disponible à l'adresse suivante : http://trade.ec.europa.eu/doclib/docs/2012/june/tradoc_149559.pdf

Commission européenne (2010), « Specific Privacy Statement, Public Consultation on the review of the scheme of generalised tariff preferences (GSP) », disponible à l'adresse suivante : http://trade.ec.europa.eu/doclib/docs/2010/march/tradoc_145976.pdf

Gindin, S. (1997), Lost and Found in Cyberspace, San Diego Law Review, disponible à l'adresse suivante : http://www.info-law.com/lost.html

Instituto Nacional de Tecnologías de la Comunicación y Agencia Española de Protección de Datos Personales (2009), « Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online », disponible à l'adresse suivante : http://www.inteco.es/Seguridad/Observatorio/Estudios/est_red_sociales_es

LRDP KANTOR Ltd (Leader) en association avec le Centre for Public Reform (2010). « Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques » – Rapport final, disponible à l'adresse suivante : http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf

Mitrano, T. (2006), A Wider World: Youth, Privacy, and Social Networking Technologies, EDUCAUSE Review, vol. 41, n° 6, disponible à l'adresse suivante : http://www.educause.edu/ero/article/wider-world-youth-privacy-and-social-networking-technologies

Perez, J.C. (2009), Facebook Will Shut Down Beacon to Settle Lawsuit, The New York Times, 19 septembre 2009, disponible à l'adresse suivante : http://www.nytimes.com/external/idg/2009/09/19/19idg-facebook-will-shut-down-beacon-to-settle-lawsuit-53916.html

Press Release/Memorandum for publication, Overview of the European Commission's referral of ACTA to the European Court of Justice, disponible à l'adresse suivante : http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc_149464.doc.pdf

Privacy International (2011), « Surveillance Monitor 2011: Assessment of surveillance across Europe », disponible à l'adresse suivante : https://www.privacyinternational.org/reports/surveillance-monitor-2011-assessment-of-surveillance-across-europe

Privacy Rights Clearinghouse, « Online Privacy: Using the Internet Safely », disponible à l'adresse suivante : http://www.privacyrights.org/fs/fs18-cyb.htm

Slazmann, V. (2000), « Are Public Records Really Public? The Collision Between the Right to Privacy and the Release of Public Court Records Over the Internet », Baylor Law Review, disponible à l'adresse suivante : http://works.bepress.com/cgi/viewcontent.cgi?article=1011&context=victoria_salzmann

Sprague, R. (2009), Rethinking Information Privacy in an Age Of Online Transparency, disponible à l'adresse suivante : http://lawarchive.hofstra.edu/pdf/academics/journals/laborandemploymentlawjournal/labor_vol25no2_sprague.pdf

York, J.C. (2011), A Case for Pseudonyms, disponible à l'adresse suivante : https://www.eff.org/deeplinks/2011/07/case-pseudonyms

6.7 Questions relatives au genre

Allen, A. (2000), Gender and Privacy in Cyberspace, Stanford Law Review Vol. 52, n°. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (mai 2000), p. 1175-1200, disponible à l'adresse suivante : http://www.jstor.org/stable/1229512

Association for Progressive Communications (2012), « Critically absent: Women in internet governance. A policy advocacy toolkit », disponible à l'adresse suivante : http://www.violenceisnotourculture.org/resources/critically-absent-women-internet-governance-policy-advocacy-toolkit

Bartow, A. (2000), « Our Data, Ourselves: Privacy, Propertization, and Gender », disponible à l'adresse suivante : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=374101

Burnett, K., Subramaniam, M., and Gibson, A. (2009), « Latinas cross the IT border: Understanding gender as a boundary object between information World », First Monday, Volume 14, Number 9, disponible à l'adresse suivante : http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2581/228

Clifford, B. (2008), « Online privacy sensitivity and gender: A case study of a highly-educated adult population », disponible à l'adresse suivante : http://gradworks.umi.com/33/36/3336862.html

EPIC, « Gender and Electronic privacy », disponible à l'adresse suivante : http://epic.org/privacy/gender/

Grubbs Hoy, M. et Milne, G. (2010), « Gender Differences in Privacy-Related Measures for Young Adult Facebook Users », disponible à l'adresse suivante : http://jiad.org/article130

VAW (2010), « Your Privacy, Your Safety », Violence Against Women Online Resources, disponible à l'adresse suivante : http://www.vaw.umn.edu/documents/internet-safety/internet-safety.html

Youn, S. et Hall, K. (2008), « Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors », disponible à l'adresse suivante : http://www.ncbi.nlm.nih.gov/pubmed/18954276

BIBLIOGRAPHIE

Alianza Regional por la Libre Expresión e Información, Saber Más III: Regional Report on Access to Information and the Protection of Personal Data (2011: Alianza Regional por la Libre Expresión e Información).

Allison, D., Protecting Human Rights in the Digital Age: Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry (2011: BSR: The Business of a Better World).

Ang, P., « The Role of Self-Regulation of Privacy and the Internet » (2011) 1 Journal of Interactive Advertising 1.

Angwin, J., & Valentino-Devries, J. (2011). Apple's iPhones and Google's Androids Send Cellphone Location. Wall Street Journal. Consulté le 13 décembre 2011 sur http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

ARTICLE 19, Written Comments in Inter-American Court of Human Rights Case n° 12.524: Jorge Fontevecchia and Hector D'amico v. Argentina (2011: ARTICLE 19, London).

Baker & MacKenzie, « A Big Year for Privacy in Greater China: 2011 Wrap Up » Newsletter: January 2012.

Banwell, L., Ray, K., Coulson, G., Urquhart, C., Lonsdale, R., Armstrong, C., Thomas, R., et al. (2004). The JISC User Behaviour Monitoring and Evaluation Framework. Journal of Documentation, 60(3), 302-320.

Beresford A. et Stajano F. (2003). « Location Privacy in Pervasive Computing », IEEE Communications Society http://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf

Biermann, Kai, (2011). « Data Protection: Betrayed by our own data ». ZEIT Online. Consulté le 1er mars 2012 (http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz).

Bits of Freedom, Contribution Bits of Freedom to the Second Universal Periodic Review of the Netherlands by the United Nations Human Rights Council (2011: Bits of Freedom, Amsterdam).

Bloustein, E. « Privacy as an aspect if human dignity: an answer to Dean Prosser » (1964) 39 NYU L Rev 962.

Boyd, D., Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the « Children's Online Privacy Protection Act ». First Monday, 16(11).

Brenton, M. (1964). The Privacy Invaders, Coward-McCann (Les Ennemis de votre vie privée. Paris : Gallimard, 1967).

BuiltWith. (2011). Google Analytics Usage Statistics – Websites using Google Analytics. Consulté le 13 décembre 2011 sur http://trends.builtwith.com/analytics/Google-Analytics

Burchell, J., « The Legal Protection of Privacy in South Africa: A Transplantable Hybrid » (2009) 13 Electronic Journal of Comparative Law 1.

Cabanellas, G., « The Right of Publicity under Argentine Law » (1998) 18 Loyola of Los Angeles Entertainment Law Review 449

Cai, L., & Chen, H. (2011). TouchLogger: inferring keystrokes on touch screen from smartphone motion. HotSec'11 Proceedings of the 6th USENIX conference on Hot topics in security (p. 9). Berkeley, CA, USA: USENIX Association.

Calcutt, D., et al., 1990. Report of the committee on privacy and related matters, Chairman David Calcutt QC, Londres : HMSO (Cmnd. 1102).

Carrasquilla, L., « Personal data protection in Latin America: retention and processing of personal data in the Internet sphere », in Bertoni, E., Ed., Towards an Internet Free of Censorship. Proposals for Latin America (2012, Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), Buenos Aires).

Carter, D. L., & Carter, J. G. (2009). The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement. Criminal Justice and Behavior, 36(12), 1323-1339.

Cavoukian, A. « Whole Body Imaging in Airport Scanners: Building in Privacy by Design » Information & Privacy Commissioner, Ontario, Canada. June 2009 http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf

Center for Democracy and Technology, Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development (2011: Center for Democracy and Technology, Washington).

Center for Democracy and Technology, Seeing Is ID'ing: Facial Recognition & Privacy (2011: Center for Democracy and Technology, Washington).

Chaos Computer Club. (2011). Chaos Computer Club analyzes government malware. Consulté le 13 décembre 2011 sur http://ccc.de/en/updates/2011/staatstrojaner

Cho, D., Real Name Verification Law on the Internet: A Poison or Cure for Privacy?, disponible à l'adresse suivante : http://weis2011.econinfosec.org/papers/Real%20Name%20Verification%20Law%20on%20the%20Internet%20-%20A%20Poison%20or%20Cu.pdf

Cirio, P., & Ludovico, A. (2011). Face-to-Facebook. Face-to-Facebook. Consulté sur www.face-to-facebook.net/theory.php

Clarke, G. (2011). Do-Not-Track laws gain US momentum. The Register. Consulté le 13 décembre 2011 sur http://www.theregister.co.uk/2011/05/06/senate_do_not_track/

Compa, E. et Bertoni, E., Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad (2010: Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), Buenos Aires).

Cooper, A. (2007). Competing on Privacy. Center for Democracy and Technology. Consulté le 13 décembre 2011 sur https://www.cdt.org/blogs/alissa-cooper/competing-privacy

Economist, (2010) « Clicking for Gold: How internet companies profit from data on the Web », in « A special report on managing information » The Economist, Volume 394, Number 8671.

Edelman, B. (2006), « Adverse Selection in Online 'Trust' Certifications » Harvard Business School, publié en ligne : http://www.benedelman.org/publications/advsel-trust.pdf

Electronic Frontier Foundation (EFF), (2011). Mobile Devices. Surveillance Self-Defense Project. Consulté le 13 décembre 2011 sur https://ssd.eff.org/tech/mobile

Electronic Privacy Information Center and Privacy International, Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments (2007: Electronic Privacy Information Center and Privacy International, États-Unis d'Amérique).

Electronic Privacy Information Center, (2011). Face Recognition. (EPIC). Consulté le 13 décembre 2011 sur https://epic.org/privacy/facerecognition/

Electronic Privacy Information Center, (2011). Personal Surveillance Technologies. Consulté le 13 décembre 2011 sur https://epic.org/privacy/dv/personal_surveillance.html

Electronic Privacy Information Center, (2011). Social Networking Privacy. Consulté le 13 décembre 2011 sur https://epic.org/privacy/socialnet/

Enders, A., Hungenberg, H., Denker, H.-P., & Mauch, S. (2008). The long tail of social networking. Revenue models of social networking sites. European Management Journal, 26(3).

EPIC, Cloud Computing, publié en ligne : http://epic.org/privacy/cloudcomputing/

EPIC, WHOIS, publié en ligne : http://epic.org/privacy/whois/

EPIC, Privacy and Consumer Profiling http://epic.org/privacy/profiling/

Commission européenne, Commission au Conseil et au Parlement européen : Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE), Bruxelles, 18 avril 2011, COM(2011) 225 final.

Commission européenne (2010). Stratégie numérique: la Commission saisit la Cour de justice d'un recours contre le Royaume-Uni en ce qui concerne la protection de la vie privée et des données à caractère personnel [IP/10/1215]. Consulté le 13 décembre 2011 sur http://europa.eu/rapid/press-release_IP-10-1215_fr.htm

European Digital Rights (EDRI), Shadow evaluation report on the Data Retention Directive (2006/24/EC) (17 avril 2011 : European Digital Rights, Bruxelles).

Parlement européen (2000). Charte des droits fondamentaux de l'Union européenne. Luxembourg : Office des publications officielles des Communautés européennes.

Facebook (2012). « Statistics » publié en ligne http://www.facebook.com/press/info.php?statistics

Fayyad, U., Grinstein, G. and Wierse, A. (2001). « Information Visualization in Data Mining and Knowledge Discovery ». Morgan Kaufman Publishers.

Federal Trade Commission, (1999) « Self-regulation and Privacy Online: A Report to Congress », mars 1999, publié en ligne : http://www.ftc.gov/os/1999/07/privacy99.pdf

Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers: Preliminary FTC Staff Report, décembre 2010.

Fernández, G., China Publishes Draft Privacy Guidelines, 14 avril 2011 (Hogan Lovells)

Filastò, A. (2011). Blue Coat device logs indicate the levels of censorship in Syria. Consulté le 13 décembre 2011 sur http://hellais.github.com/syria-censorship/

Filippi, P. de (2011). Notes on Privacy in the Cloud.

Fitzpatrick, M. « Mobile that allows bosses to snoop on staff developed » BBC News 10/03/2010 http://news.bbc.co.uk/1/hi/technology/8559683.stm

Flaherty, D. H. (1999). Visions of Privacy: Past, present and future. Visions of privacy: policy choices for the digital age (p. 19-38). University of Toronto Press.

Fuchs, C. (2009). Social networking sites and the surveillance society a critical case study of the usage of studiVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance. Salzbourg : Forschungsgruppe Unified Theory of Information.

Gates, J., & Privacy Working Group (1995). Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information. Information Policy Committee, Information Infrastructure Task Force. Consulté sur http://aspe.hhs.gov/datacncl/niiprivp.htm

Gellman, R., & World Privacy Forum (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Consulté sur http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Google (2008). Google Zeitgeist 2008. Consulté le 13 décembre 2011 sur https://www.google.com/intl/en/press/zeitgeist2008/world.html#top

Google (2011). Google Transparency Report. Google. Consulté le 13 décembre 2011 sur https://www.google.com/transparencyreport/

Gorge, M. (2008). Data protection: why are organisations still missing the point? Computer Fraud & Security, 2008(6), 5-8. doi:10.1016/S1361-3723(08)70095-2.

Greenleaf, G., « Asia-Pacific data privacy: 2011, year of revolution? » [2011] UNSWLRS 30

Greenleaf, G., The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, University of New South Wales Faculty of Law Research Series, Paper 42, 2011.

Griffiths, J. (n.d.). Student searching behaviour and the Web: use of academic resources and google. Library trends, 2005, vol. 53, n° 4, pp. 539-554, https://www.ideals.illinois.edu/bitstream/handle/2142/1749/Griffiths539554.pdf?sequence=2

Hargittai, E. (2010). Trust online: young adults' evaluation of Web content. International Journal of Communication, 4.

Higginbotham, S. (2010). iPhone 4 Sensors Highlight a Bright Spot for VCs. GigaOM. Consulté sur http://gigaom.com/2010/06/08/iphone-4-sensors-highlight-a-bright-spot-for-vcs/

Hilles, L., & Jugendschutz.Net. (2011). Verlockt – Verlinkt – verlernt? Werbung, Vernetzung und Datenabfragen auf Kinderseiten. Mainz, Allemagne.

Conseil des droits de l'homme (2009), Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement : Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Martin Scheinin. Conseil des droits de l'homme, Treizième session, Point 3 de l'ordre du jour. 28 décembre 2009, A/HRC/13/37 http://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/05/pdf/G0917805.pdf?OpenElement

Hunton & Williams, Client Alert, janvier 2010. Disponible à l'adresse suivante : http://www.hunton.com/files/News/4bfa5361-4d8f-4c7e-af03-75055a82202c/Presentation/NewsAttachment/7d2612ba-40d6-4884-83de-c01965341d41/new_chinese_tort_liability_law.pdf

Initiative Vorratsdatenspeicherung (2011). Stoppt die Vorratsdatenspeicherung. Consulté le 13 décembre 2011 sur https://www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html

Commission interaméricaine des droits de l'homme, Rapport sur la situation des défenseurs des droits de l'homme dans les Amériques. Disponible à l'adresse suivante : http://www.cidh.oas.org/pdf%20files/DEFENDERS%20FRENCH%20COMPLETE.pdf

Introna, L. D., & Nissenbaum, H. F. (2009). Facial Recognition Technology: A Survey of Policy and Implementation Issues. SSRN eLibrary. SSRN. doi:10.2139/ssrn.1437730.

Union internationale des télécommunications (UIT), 2010. Measuring the Information Society. [en ligne] http://www.itu.int/ITU-D/ict/publications/idi/material/2012/MIS2012_without_Annex_4.pdf

Kilkelly, U., Le droit au respect de la vie privée et familiale : Un guide sur la mise en œuvre de l'article 8 de la Convention européenne des droits de l'homme. Précis sur les droits de l'homme, n° 1 (2003 : Direction générale des droits de l'homme, Conseil de l'Europe, Strasbourg).

King, E. (2011). Our response to EU consultation on legality of exporting surveillance and censorship technology. Privacy International. Consulté le 13 décembre 2011 sur https://www.privacyinternational.org/reports/our-response-to-the-eu-consultation-on-legality-of-exporting-surveillance-and-censorship

Koops, B., and Sluijs, J., Network Neutrality and Privacy According to Art. 8 ECHR, Tilburg Law School Legal Studies Research Paper Series n° 017/2011.

La Rue, F. (2011). Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Frank La Rue. 2010 : Conseil des droits de l'homme [A/HRC/14/23]. Genève : Organisation des Nations Unies.

Leon, P., Ur, B., Balebako, R., Cranor, L., Shay, R., and Wang, Y., Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising (2011: Carnegie Mellon University, Pittsburgh).

Leong, F. and Bakar, H., « Personal Data Protection Act 2010 » (July-September 2010) Legal Herald 1.

Lessig, L. (1999). « Code and Other Laws of Cyberspace » Basic Books, New York.

Marinos, L., & Agence européenne de cyber-sécurité (2011). Cyber-bullying and online grooming: helping to protect against the risks. Héraklion, Grèce.

Marsh, R., « Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet » (2009) 15 Michigan Telecommunications and Technology Law Review 543

Mayer, J. (2011). Tracking the Trackers: Microsoft Advertising. Center for Internet and Society (CIS), Stanford Law School. Consulté le 13 décembre 2011 sur http://cyberlaw.stanford.edu/node/6715

McKenzie, P. Dicker, A., et Fang, J., China Issues New Guidelines on Data Privacy Protection, 11 avril 2011 (Morrison Foerster).

McKenzie, P., and Milner, G., China Update, March 2009: Recent Developments in Data Protection, 9 mars 2009 (Morrison Foerster).

McKenzie, P., and Milner, G., Data Privacy in China: Criminal Law Developments, 25 janvier 2010 (Morrison Foerster).

Mueller, M. (2011). DPI Technology from the standpoint of Internet governance studies: An introduction. Syracuse University. Consulté sur http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

Mueller, M. L. (2010). Networks and States: The Global Politics of Internet Governance (p. 280). MIT Press.

Mueller, P. (2011). Offene Staatskunst – Strategie für eine vernetzte Welt. Arbeitskreis Internet Governance. Munich, Allemagne : Münchner Centrum für Governance-Forschung (MCG).

Netter, W. « The Death of Privacy » Privacy Module I: Data Profiling Introduction, University of Harvard, 2002 http://cyber.law.harvard.edu/privacy/Module2_Intro.html

Niemietz v Germany (1992), 16 EHRR 97.

Ong, R., « Recognition of the right to privacy on the Internet in China » (2011) 1 International Data Privacy Law 172.

Padania, S., Gregory, S., Alberdingk-Thijm, Y., & Nunez, B. (2011). Cameras Everywhere Report 2011. Consulté sur http://www.witness.org/cameras-everywhere/report-2011

Pang, D., Chen, B., & Lee, D. (2008). Eight now held in internet sex probe. The Standard. Consulté le 13 décembre 2011 sur http://www.thestandard.com.hk/news_detail.asp?pp_cat=12&art_id=61125&sid=17431562&con_type=3#

Pomfret, J. (2009). Technician guilty in Edison Chen sex pictures trial. Victoria News. Consulté le 13 décembre 2011 sur http://www.vicnews.com/entertainment/television/43998412.html

Privacy Foundation, 9 juillet 2001 http://www.sonic.net/~undoc/extent.htm

Privacy International, (2006) « Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments » http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65435&als[theme]=Privacy%20and%20Human%20Rights

Privacy International, 1996, ID Card Frequently Asked Questions https://www.privacyinternational.org/article/id-card-frequently-asked-questions

Privacy International (2006). Privacy International 2006 - Executive Summary. Consulté le 13 décembre 2011 sur https://www.privacyinternational.org/article/phr2006-executive-summary

Privacy International (2011). United Kingdom – Privacy Profile. Privacy International. Consulté le 13 décembre 2011 sur https://www.privacyinternational.org/article/united-kingdom-privacy-profile

Privacy Rights Clearinghouse (2010), « Fact Sheet 18: Privacy and the Internet: Traveling in Cyberspace Safely », publié en ligne http://www.privacyrights.org/fs/fs18-cyb.htm

Reding, V. 2010, Next steps for Justice, Fundamental Rights and Citizenship in the EU European Policy Centre Briefing Brussels, 18 mars 2010, Bruxelles. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/108

Robertson, D. S. (1998). The New Renaissance: Computers and the Next Level of Civilization (p. 208). Oxford University Press, États-Unis d'Amérique.

Robinson, N., Graux, H., Botterman, M., and Valieri, L., Review of EU Data Protection Directive: Summary, prepared for the UK Information Commissioner's Office, mai 2009.

Rooney, B. (2011). U.K. Publishes EU « Cookie » Directive Guidelines. Wall Street Journal. Consulté le 13 décembre 2011 sur http://blogs.wsj.com/tech-europe/2011/05/09/u-k-publishes-e-u-cookie-directive-guidelines/

Ross, L., Gao, K. et Zhou, A., China Issues Draft Guidelines on Online Privacy, Announces new Agency to Supervise the Internet, 19 mai 2011 (Wilmer Hale).

Rotenburg M. et Hoofnaglem C. « Submission to the House Government Reform Committee on Data Mining », 25 mars 2003. http://epic.org/privacy/profiling/datamining3.25.03.html

Schulman, A. « The Extent of Systematic Monitoring of Employee E-mail and Internet Use »

Scott, J. C. (1998). Seeing like a state : how certain schemes to improve the human condition have failed. New Haven: Yale University Press.

Senior, A., & Pankanti, S. (2011). Privacy protection and face recognition. In S. Z. Li & A. K. Jain (Eds.), Handbook of Face Recognition. Springer.

Shaker, L. (2006, April 3). In Google we trust: Information integrity in the digital age. First Monday. Ghosh, Rishab Aiyer. Consulté sur : http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1320/1240

Silva, A., « Personal Data Protection and Online Services in Latin America » in Bertoni, E., Ed., Towards an Internet Free of Censorship. Proposals for Latin America (2012, Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), Buenos Aires).

Silver, V., & Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. Bloomberg. Consulté le 28 août 2011 sur http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

Soghoian, C. (2007) « The Problem of Anonymous Vanity Searches » Indiana University Bloomington – School of Informatics. Publié en ligne http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953673

Solove, D.J. (2008) Understanding Privacy Harvard University Press.

Sonne, P., & Coker, M. (2011). Foreign Firms Helped Gadhafi Spy on Libyans. Wall Street Journal. Consulté le 23 septembre 2011 sur http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

South African Law Reform Commission, Project 124: Privacy And Data Protection Report (2009: South African Law Reform Commission).

Stewart, B. (2004). A comparative survey of data protection authorities. Privacy Law and Policy Reporter, 11(2).

Stuart, K. (2011). PlayStation Network hack: what every user needs to know. The Guardian. Consulté le 13 décembre 2011 sur http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/psn-security-advice

Sung-jin, Y. (2011). 35m Cyworld, Nate users' information hacked. The Korea Herald. Consulté le 13 décembre 2011 sur http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110728000881

Sweeney, L. « Strategies for De-Identifying Patient Data for Research » Carnegie Mellon University, Data Privacy Lab, 1998 http://www.ocri.ca/ehip/2005/presentations/Sweeney_bw.pdf

Telecommunications Research Centre (2011). World telecommunication. Genève : UIT.

The Economist, (2010). « New Rules for Big Data », in « A special report on managing information » The Economist, Volume 394, Number 8671.

TRUSTe, (2009). « TRUSTe Press Releases and Facts », publié en ligne http://www.truste.com/about_TRUSTe/press-room.html

Tufekci, Z. (2010). Facebook: The Privatization of our Privates and Life in the Company Town. Technosociology: Our Tools, Ourselves. Consulté le 13 décembre 2011 sur http://technosociology.org/?p=131

ONU, Comité des droits de l'homme, Observation générale n° 16 : Le droit au respect de la vie privée, de la famille, du domicile et de la correspondance, et le droit d'être protégé contre les atteintes à l'honneur et à la réputation (art. 17), adoptée le 4 août 1988.

Valentino-Devries, J., Sonne, P., & Malas, N. (2011). Blue Coat Acknowledges Syria Used Its Gear for Internet Censorship Amid Arab Spring. Wall Street Journal. Consulté le 13 décembre 2011 sur http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

Vasile, J. (2011). Presentation of the FreedomBox. Elevate 2011 - Music, Arts and Political Discourse. Graz, Autriche : Verein zur Förderung des gesellschaftspolitischen und kulturellen Austausches.

Volio, F. « Legal Personality, Privacy and the Family » in Henkin (ed), The International Bill of Rights (Columbia University Press 1981).

W3Techs. (2011). Usage Statistics and Market Share of Traffic Analysis Tools for Websites. Q-Success Web-based Services. Consulté le 13 décembre 2011 sur http://w3techs.com/technologies/overview/traffic_analysis/all

Warren, S. and Brandeis, L., « The Right to Privacy » (1890) 4 Harvard Law Review 193

Weber, T. Cybercrime threat rising sharply, BBC News, 31/01/09 http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

Westin, A. (1967) « Privacy and Freedom » Atheneum, New York.

Workman, R., « Balancing the Right to Privacy and the First Amendment » (1992) 29 Houston Law Review 1059.

York, J. C. (2010). Policing Content in the Quasi-Public Sphere. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University.

ENTRETIENS

M. Guo Liang, Directeur du China Internet Project et membre du Groupe consultatif multipartite auprès du Secrétaire général de l'ONU pour le Forum sur la gouvernance d'Internet, Académie chinoise des sciences sociales, Chine

M. Yang Wang, Ph.D., chercheur, CyLab, Université Carnegie Mellon, États-Unis

Mme Ceren Unal, LL.M., Département de droit civil, Faculté de droit de l'Université Bilkent

M. Ang Peng Hwa, expert du droit de l'Internet de Singapour. Directeur du Centre de recherches sur l'Internet de Singapour

M. Erick Iriarte Ahon, expert latino-américain de la protection de la vie privée. Observateur en Amérique latine

Katitza Rodriguez, Directrice pour les droits internationaux, EFF

Karen Reilly, Directrice pour les politiques publiques, Projet TOR

Ali G. Ravi, TacticalTech

Moez Chackchouk, Association tunisienne de l'Internet, ATI

Primavera de Filippi, Université Panthéon-Assas, Paris II

Peter Parycek, Directeur du Centre pour l'administration en ligne, Donau-Universität, Krems

Robert Bodle, Uni Mount Joseph

Sameer Padania, Macroscope et Witness

Peter Bradwell, Open Rights Group

Ulrike Höppner, Johann Wolfgang Goethe-Universität, Francfort

Source anonyme, ancien employé d'une grande entreprise technologique

Source anonyme, ancien employé d'une grande entreprise technologique

Source anonyme, ancien employé d'une grande entreprise technologique

Eduardo Bertoni, Directeur du Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Argentine

M. Hong Xue, professeur de droit, Directeur de l'Institut de politique et de droit de l'Internet (IIPL), Université de pédagogie de Beijing

Monique Fanjoy, responsable des nouveaux médias, Commissariat à la protection de la vie privée du Canada

Abu Bakar Munir, professeur de droit, Faculté de droit, Université de Malaya, Malaisie

Joe McNamee, Coordonnateur des activités de plaidoyer auprès de l'UE, European Digital Rights

Amr Gharbeia, Egyptian Initiative for Personal Rights

Jamie Horsley, maître de recherche et professeur de droit, Yale Law School, Directeur adjoint, The China Law Center

Nepomuceno Malaluan, Codirecteur, Institute for Freedom of Information, Philippines

Cynthia M. Wong, Directeur, Global Internet Freedom Project, Center for Democracy & Technology

Sinfah Tunsarawuth, juriste et auteur indépendant spécialisé dans les médias, Bangkok, Thaïlande

Prim Ot van Daalen, Directeur, Bits of Freedom, Pays-Bas

Sunil Abraham, Directeur, Centre for the Internet and Society, Inde

APPENDICE 1 : SIGLES ET ACRONYMES

APEC	Coopération économique Asie-Pacifique
CNIL	Commission nationale de l’informatique et des libertés
COPPA	Loi sur la protection de la vie privée des enfants
DPAI	Autorité indienne de protection des données
DPI	Inspection approfondie des paquets
DSF	Digital Signage Federation
DUDH	Déclaration universelle des droits de l’homme
ECPA	Loi sur la confidentialité des communications électroniques
EDRI	European Digital Rights
EFF	Electronic Frontier Foundation
ENISA	Agence européenne de cybersécurité
EPIC	Electronic Privacy Information Center
FAI	Fournisseur d’accès à l’Internet
FMI	Fonds monétaire international
FTC	Federal Trade Commission
GNI	Initiative mondiale des réseaux
GPS	Système de positionnement global
IMEI	Numéro international d’identification d’appareil mobile
IMSI	Numéro identificateur d’usager mobile
IP	Protocole Internet
LLU	Dégroupage de la boucle mobile
MENA	Moyen-Orient et Afrique du Nord
NAI	Network Advertising Initiative
OCDE	Organisation de coopération et de développement économiques
OEA	Organisation des États américains

OMB	Bureau de la gestion et du budget
OSCE	Organisation pour la sécurité et la coopération en Europe
OSP	Fournisseur de services en ligne
PIDCP	Pacte international relatif aux droits civils et politiques
POPAI	Point of Purchase Advertising International
RFID	Identification par radiofréquence
TRAI	Autorité indienne de régulation des télécommunications

APPENDICE 2 : LISTE DES FIGURES ET DES ENCADRÉS

L'UNESCO, aux termes de son Acte constitutif, promeut « la libre circulation des idées, par le mot et par l'image » et s'est engagée à faciliter la mise en place d'un espace Internet libre, ouvert et accessible dans le cadre de la promotion d'une liberté d'expression complète en ligne et hors ligne. Nous espérons que cette publication fournira aux État membres de l'UNESCO et autres parties prenantes, nationales et internationales, un outil de référence utile. Nous voudrions que cette publication contribue à réunir les parties prenantes pour un débat éclairé sur les approches qui favorisent le respect de la vie privée sans compromettre la liberté d'expression. Dans les années qui viennent, l'UNESCO cherchera spécifiquement à diffuser des informations sur les bonnes pratiques et la collaboration internationale concernant les points d'intersection entre liberté d'expression et respect de la vie privée. La recherche sur la sauvegarde du principe de la liberté d'expression dans la politique de l'Internet sur un large éventail de questions restera un élément du mandat normatif de l'UNESCO et de ses conseils techniques aux parties prenantes.

Jānis Kārkliņš
Sous-Directeur général pour la communication et l'information, UNESCO

Toby Mendel • Andrew Puddephatt • Ben Wagner • Dixie Hawtin • Natalia Torres

COLLECTION UNESCO SUR LA LIBERTÉ DE L'INTERNET
Secteur de la communication et de l'information
Organisation des Nations Unies
pour l'éducation, la science et la culture





Organisation
des Nations Unies
pour l'éducation,
la science et la culture

Secteur
de la communication
et de l'information

